



410 - Is Privacy the Next Superfund? How to Navigate Privacy & Data Security Issues

Jon Leibowitz
Commissioner
Federal Trade Commission

Nuala O'Connor Kelly
Chief Privacy Leader & Senior Counsel
General Electric Company

Christine Varney
Partner
Hogan & Hartson LLP

Faculty Biographies



Jon Leibowitz

Jon Leibowitz is a commissioner of the Federal Trade Commission in Washington, DC.

In joining the Commission, Mr. Leibowitz resumed a long career of public service. In the past he was the Democratic chief counsel and staff director for the U.S. Senate antitrust subcommittee, where he focused on competition policy and telecommunications matters. He served as chief counsel and staff director for the Senate subcommittee on terrorism and technology and the Senate subcommittee on juvenile justice. In addition, he served as chief counsel to Senator Herb Kohl. Mr. Leibowitz also worked for Senator Paul Simon. In the private sector, Mr. Leibowitz served most recently as vice president for congressional affairs for the Motion Picture Association of America and worked as an attorney in private practice in Washington.

He has co-authored amicus briefs before the U.S. Supreme Court on issues ranging from gun control to the census.

He is a Phi Beta Kappa graduate of the University of Wisconsin with a B.A. and he graduated from the New York University School of Law.

Nuala O'Connor Kelly
Chief Privacy Leader & Senior Counsel
General Electric Company

Christine Varney

Christine Varney rejoined Hogan & Hartson, after five years in government service, to head the firm's Internet practice group. This practice provides full service assistance to companies doing business globally, including providing advice on antitrust, privacy, business planning and corporate governance, intellectual property, and general liability issues. Ms. Varney also provides antitrust, competition policy, and regulatory advice to a variety of companies. Ms. Varney's clients have included such companies as eBay, Fox Interactive Media/MySpace, Ernst & Young, Zango, DoubleClick, Washingtonpost, Newsweek Interactive, Dow Jones & Company, AOL, Synopsys, Compaq Computer, Gateway, Netscape, The Liberty Alliance, and Real Networks.

Before rejoining the firm, she served as a federal trade commissioner. At the FTC, she led the government's effort to examine privacy issues in the information age, resulting in congressional and agency hearings, proposed industry standards, and increased government enforcement of laws protecting privacy. She also pioneered the application of innovation market theory analysis to transactions in both electronic high technology and biotechnology.

Prior to becoming a federal trade commissioner, she was an assistant to the president and secretary to the Cabinet. She was the primary point of contact for the 20-member Cabinet, responsible for the overall coordination of several major issues and initiatives between the White House and various agencies.

Christine Varney
Partner

PRIVACY BRIEFING MATERIAL

Association of Corporate Counsel

October 29 – 31, 2007



may not have been arrested or charged with crimes, as well as access to case files, which often contain erroneous or unproved allegations. OneDOJ illustrates the ongoing tensions between law enforcement and personal privacy concerns that have been evidenced so often this past year.

Articles on this issue are available at: <http://www.washingtonpost.com/wp-dyn/content/article/2006/12/25/AR2006122500483.html> and <http://www.securityfocus.com/brief/396>

The Hogan & Hartson Privacy Team compiles a bi-monthly real-time update of privacy, security, and consumer protection activities. Following, for your reference, is a compendium of those briefings covering the first half of 2007..

Please contact any member of the H&H Privacy Team if you would like more information: http://www.hhlaw.com/PracticeAreas/areas_professionals.aspx?op=&firmService=111

December 19, 2006 – January 8, 2007.

I. PRIVACY

- **Microsoft Announces Behavioral Targeting** – Microsoft has begun linking users' search activity on various Microsoft sites with personal information provided by users when they sign up for Hotmail email and other Microsoft services. Microsoft then uses the compiled information to build profiles for classes of users and sell marketers the opportunity to send ads to targeted groups as they search Microsoft sites. Microsoft rolled out its behavioral targeting technology in September, after a year of testing, and now plans to expand its use around the world. Microsoft found that behavioral targeting increased the likelihood that a person would click on an ad by as much as 76%. Privacy advocates worry about companies compiling so much information about their customers, but Microsoft and others engaged in behavioral targeting counter that the user's experience is more positive when they see only targeted ads.

An article on this issue is available at: <http://www.azcentral.com/business/articles/1230biz-microsoft1230.html>

- **DOJ Database Raises Privacy Concerns** – The *Washington Post* reports that the Department of Justice (DOJ) is building a database that will standardize the formats and means of accessing case files from the FBI, Drug Enforcement Administration, and other federal law enforcement agencies. The files include investigative reports, criminal histories, details of offenses, and the names, addresses, and other information of criminal suspects or targets. Law enforcement officials believe the system, known as "OneDOJ," is an important step toward improved information sharing with local law enforcement. Privacy and civil-liberties advocates have voiced concern that such a system provides local police officers around the country with access to personal details about people who

- **Study Shows that Most MySpace Users Understand Privacy Concerns** – A recent study conducted by two criminal justice professors looked at 1,475 randomly-chosen teenage profiles on MySpace.com. The study found that 91% of the profiles did not list full names and about 40% of the profiles were set to private and only viewable by friends. However, the study did find that 5% of the teenagers posted pictures of themselves in bathing suits or underwear, and 15% showed friends in such attire. The researchers emphasized the benefits to users from having MySpace profiles, including learning HTML coding and gaining a sense of identity and self-esteem. These results appear to indicate that while there may still be work to be done, the efforts by law enforcement, lawmakers, and the social networking companies may be generating results in terms of users' heightened awareness of privacy concerns.

An article on this issue is available at: http://www.usatoday.com/tech/news/2007-01-05-myspace-responsible_x.htm

II. SECURITY

- **Federal Identity Theft Task Force Seeks Public Comments** – The Federal Identity Theft Task Force ("Task Force") is soliciting public comments on the steps the government can take to reduce identity theft. The task force is considering several proposals that could directly impact companies that collect and use personal information, including:
 - investigating how Social Security Numbers ("SSNs") are being used by the private sector and how these uses could be modified to reduce the exposure of SSNs;
 - recommending that national data security requirements be imposed on all companies that maintain sensitive customer information; and
 - recommending the creation of a federal breach notification requirement.

The Task Force previously released a set of interim recommendations. While that document focused exclusively on what government agencies can and should do to fight identity theft, the upcoming recommendations will likely include suggestions for the private sector and may call for targeted legislative or regulatory intervention.



Comments are due by January 19 and can be filed by e-mail at Taskforcecomments@idtheft.gov or via mail or hand delivery to the Federal Trade Commission.

A copy of the request for comment is available at <http://www.ftc.gov/speeches/majoras/061221PublicNoticeFinal.pdf>

The Task Force's website is available at: <http://www.ftc.gov/bcp/edu/microsites/idtheft/taskforce.htm>

- **Data Breaches and Consumer Complaints Continue** – There has been significant media coverage of the Privacy Rights Clearinghouse's announcement that since the ChoicePoint breach in February 2005, over 100 million records containing personal information have been lost or stolen. These headlines along with recent breaches at Boeing, University of Texas at Dallas, and Aetna will keep data breach legislation on lawmakers' 2007 agenda as the 110th Congress gets underway. Legislative and regulatory attention will also be driven by consumer unrest. The FTC, which has already been active in this area, said it received 255,000 complaints about identity theft in 2005, accounting for more than a third of all of the complaints received by the Commission.

An article on this issue is available at: <http://www.nytimes.com/2006/12/18/technology/18link.html?ex=1168405200&en=48e2483307d5abe8&ei=5070>

An FTC press release on complaints received by the agency is available at: <http://www.ftc.gov/opa/2006/01/topten.htm>

III. SPYWARE

- **Sony BMG Settles Anti-Piracy/Spyware Suits with Texas and California** – Sony BMG has agreed to pay \$1.5 million to Texas and California and refund thousands more to consumers in refunds for damage resulting from an anti-piracy program loaded onto their computers by hidden software on Sony BMG CDs and from recommended attempts to remove the program. The software was originally designed to prevent piracy by limiting the number of copies that could be made of the CD, but the program loaded onto consumers' computers also allegedly reported information back to Sony BMG when played on Internet-enabled computers and instructions on how to remove the program are also alleged to have damaged users' computers. The settlement requires Sony BMG to pay each state \$750,000 and to reimburse consumers whose computers were damaged attempting to remove the anti-piracy program.

Sony BMG's settlement with the State of Texas is available at: http://www.oag.state.tx.us/newspubs/releases/2006/121406sony_afj.pdf.
Sony BMG's settlement with the State of California is available at: http://ag.ca.gov/cms_pdfs/press/2006-12-19_Settlement_Judgment.pdf.



IV. STATES – ALL ISSUES

- **States Continue to Enact Identity Theft Legislation** – As reported in the *Privacy and Data Security Briefing* throughout the past year, a flurry of state legislation addressing identity theft was enacted in 2006 and went into effect on January 1, 2007 with more likely on the way. Businesses in three states, Arizona, Hawaii, and Utah, are now subject to breach notification laws that went into effect with the start of the new year. These new statutes bring the total number of states that have enacted breach notification legislation to 33.

Links to each state's 2006 breach notification legislation are available at: <http://www.ncsl.org/programs/lis/cip/priv/breach06.htm>.

In addition, eight states saw credit freeze laws take effect at the beginning of the year. These states (Hawaii, Illinois, Kansas, New Hampshire, Oklahoma, Pennsylvania, Rhode Island, and Wisconsin) join a group of 26 states that have enacted some form of credit freeze legislation.

Links to each state's 2006 credit freeze legislation are available at: http://www.ncsl.org/programs/banking/SecurityFreeze_2006.htm.

- **Michigan Enacts Breach Notification Bill** – Governor Jennifer Granholm (D) signed legislation on January 3, 2007 that would provide penalties of up to \$750,000 per breach for businesses failing to notify individuals whose personal information was compromised. Under the Act, notification is triggered when substantial loss or identity theft is likely to result. However, entities that have implemented breach notifications pursuant to and in accordance with Gramm-Leach-Bliley and HIPAA are exempt from the notice requirements. Michigan will join a current total of 33 states requiring breach notification when the act goes into effect on July 2, 2007.

A copy of the Act is available at: [http://www.legislature.mi.gov/\(S\(cvnimeftjwvljfcgcuoyysvg\)\)/documents/2005-2006/publicact/htm/2006-PA-0566.htm](http://www.legislature.mi.gov/(S(cvnimeftjwvljfcgcuoyysvg))/documents/2005-2006/publicact/htm/2006-PA-0566.htm).

A press release from the State of Michigan regarding the Act is available at: <http://www.mi.gov/som/0,1607,7-192--159364--,00.html>.

V. SPAM

- **2006 Reports Highlight Rise in Spam** – As 2006 came to a close, numerous end-of-year reports revealed that spam is on the rise leading some to suggest that CAN-SPAM was merely a symbolic gesture with little actual effect.



According to a report by Ferris Research, in 2006, spam-related costs resulting in lost productivity and efforts to thwart the receipt of spam cost an estimated \$17 billion in the United States and close to \$50 billion worldwide. The holiday season was a particularly bad time for e-mail recipients with 93 percent of e-mail from September through November consisting of spam, as stated in a Postini report. IronPort Systems provided similar findings concluding that spam volumes increased 35 percent in the month of November.

The reports also identified an increase in image spam. This spam (which replaces text with images so as to avoid text-focused spam-filtering software) accounted for 30 percent of junk e-mails in 2006 compared with just 2 percent in 2005. IronPort reported that image spam peaked at 25 percent of total spam volume in October, compared to 4.8 percent last year. In addition to image spam, botnet use is blamed as a leading cause for the rise in spam.

Also escalating in 2006 were phishing scams. A report originating from the United Kingdom found that online banking fraud through phishing increased 50 percent in the first quarter of 2006.

Ultimately, this increase in spam and phishing e-mails will affect all companies that rely on commercial e-mail to reach consumers. These companies will face new technology solutions designed to combat spam that may limit delivery of legitimate e-mails as well as lead to greater consumer wariness of purported commercial e-mail communications.

Articles highlighting the rise in spam and related recent reports are available at: http://today.reuters.com/news/articlenews.aspx?type=internetNews&storyID=2006-12-20T214010Z_01_N19314994_RTRUKOC_0_US-WORK-SPAM.xml&pageNumber=0&imageid=&cap=&sz=13&WTModLoc=NewsArt-C1-ArticlePage2; <http://www.ecommercetimes.com/story/54895.html> and http://www.infoworld.com/article/06/12/28/HNspamunstopable_1.html

- **Companies Ignoring EU E-mail Privacy Law** – A recent report issued by data and marketing company CDMS concluded that more than one third of top companies in the United Kingdom are failing to comply with European Union (“EU”) laws related to unsolicited commercial e-mails. Under the three-year-old EU directive on privacy and electronic communications, Internet users have the right not to receive commercial e-mails. Commentators note that the failure of these companies to comply with laws relating to commercial e-mails creates the real risk that they will tarnish their reputations.

An article announcing this report is available at: http://icwales.icnetwork.co.uk/0300business/0100news/tm_headline=top-firms--ignore--email-privacy-law-%26method=full%26objectid=18382458%26siteid=50082-name_page.html.



- **Another Government Agency Warns of Recent Phishing Scam** – The IRS is the latest government agency to have its name used in a phishing scam. In this case, the phishers claim to be the IRS and offer recipients a refund. These types of scams are expected to increase as tax season approaches.

An article about this development is available at: <http://www.poughkeepsiejournal.com/apps/pbcs.dll/article?AID=/20070104/BUSINESS/70103035>

VI. GRAMM-LEACH-BLILEY ACT

- **SEC Sets April Goal for Proposed Revisions to Gramm-Leach-Bliley Notices** – In its semiannual regulatory report, the Securities and Exchange Commission (“SEC”) said it hopes to issue a notice of proposed rulemaking (“NPRM”) in April suggesting revisions to the notices financial institutions are required to send their customers under the Gramm-Leach-Bliley Act. The NPRM, which would be jointly issued with the Federal Trade Commission and several banking regulatory agencies, would provide companies with the opportunity to comment on the proposed changes. In December 2003, the agencies issued an advance notice of proposed rulemaking that solicited the private sector’s input on the need for, and form and content of, alternate privacy notices.

A copy of the SEC’s notice is available at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2006_unified_agenda_&docid=f:ua061059.pdf

The advance notice of proposed rulemaking is available at: http://www.ftc.gov/privacy/privacyinitiatives/financial_rule_inrp.html

VII. INTERNATIONAL ACTIVITIES

EU – Bulgaria and Romania Joined the European Union on January 1, 2007 – On January 1, 2007, Bulgaria and Romania became member states of the EU, bringing the number of countries that are members of the EU to 27. By joining the EU, Romania and Bulgaria also become members of the European Economic Area (“EEA”), a grouping of countries that consists of the 27 European Union Member States and three of the four Member States of the European Free Trade Area, commonly known as EFTA (Iceland, Liechtenstein, and Norway).

For information on all EU Member States, see: http://europa.eu/abc/european_countries/eu_members/index_en.htm

VIII. RADIO FREQUENCY IDENTIFICATION TECHNOLOGIES (RFID)

- **IBM Announces Release of RFID Middleware** – IBM recently announced its release of the WebSphere RFID Information Center (“RFID Information Center”), a data



repository that was developed according to the Electronic Product Code Information Service ("EPCIS") standards that are expected to be approved at the end of January. The RFID Information Center, which consists of a data server, a shipment verification tool, and an EPCIS-based data-exchange component, allows RFID data to be aggregated, analyzed, and shared among the various participants in the supply chain. In the pharmaceutical industry, for example, the RFID Information Center will allow the secure sharing of data among manufacturers, distributors, hospitals and pharmacies thereby facilitating the detection of any counterfeit or expired drugs and minimizing product loss in the supply chain.

The RFID Information Center is available now and is currently being tested in several industries including pharmaceuticals and consumer packaged goods.

An article discussing the product is available at:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=9&articleId=9006989&intsrc=hm_topic

January 8, 2007 – January 22, 2007.

I. PRIVACY

- **Attorney General Indicates Continued Interest in Data Retention Legislation** – Attorney General Alberto Gonzales stated in a hearing before the Senate Judiciary Committee on January 18, 2007, that the Bush administration is continuing to explore data retention legislation that would require ISPs to retain records of customers' online activity. Rep. Diana DeGette (D-CO) was a proponent of such legislation in the last Congress, and according to an aide, plans to advance data retention legislation this year. As discussed in previous *Privacy and Data Security Briefings*, privacy advocates object to imposing data retention requirements on ISPs. We will monitor the progress of any data retention legislation that may be introduced in this session of Congress.

An article on this issue is available at:
http://news.com.com/Attorney+general+to+talk+data+retention+with+new+Congress/2100-1036_3-6151325.html.

- **Senators Promise to Review Government Data Mining Programs** – The first hearing of the Senate Judiciary Committee discussed the possible privacy threats at issue in federal data mining programs. Senator Patrick Leahy (D-VT), Chairman of the Committee, stated that he plans to hold a series of hearings on privacy-related issues during this session of Congress. Leahy also stated that data mining programs, which are used frequently throughout federal agencies, may have value but "often lack adequate safeguards to protect privacy and civil liberties." Senator Russ Feingold (D-WI), with Senators Leahy, Daniel Akaka (D-HI) and John Sununu (R-NH), reintroduced a bill



called the Federal Agency Data Mining Reporting Act (S. 236), which would require, among other things, the heads of federal agencies engaged in data mining to submit a report to Congress on many aspects of the program.

An article on this issue is available at:
http://news.com.com/Senators+pledge+scrutiny+of+federal+data+mining/2100-1028_3-6149118.html?tag=nefd.top.

The text of S. 236 is available at: http://thomas.loc.gov/cgi-bin/t2GPO/http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:s236is.txt.pdf

- **Court Rules No Constitutionally Protected Privacy Interest in Social Security Numbers Involved in Identity Theft** – The United States District Court for the Southern District of Ohio recently held that an identity theft victim who demonstrated financial and reputational harm did not have a federally protected constitutional right to privacy in her Social Security number. The court reviewed other federal cases involving privacy generally and privacy and Social Security numbers specifically and concluded that the individual interest at stake must implicate a fundamental right in order to be protected by the constitutional right to privacy. Other cases that found Social Security numbers to be protected by a constitutional right to privacy involved threats to the personal security of the individual. The court found that the financial and reputational harm suffered by the plaintiff in this case was not equivalent to that type of harm. The court therefore granted the defendants' motion to dismiss the plaintiff's constitutional claims.

A copy of the court's decision in *Lambert v. Hartmann*, S.D. Ohio (Dec. 29, 2006) is available at: <http://cases.n.stuff.googlepages.com/Lambert-v-Hartmann.pdf>.

II. SECURITY

- **Feinstein Reintroduces Data Breach Notification Bill** – Senator Diane Feinstein (D-CA) introduced S. 239, the "Notification of Risk to Personal Data Act" on January 10. The bill is similar to legislation that Feinstein introduced in the 109th Congress and that was eventually incorporated into S.1789, which was one of two breach notification bills that passed out of Committee in the Senate last year. Given Senator Feinstein's prominent role in this debate last year, we expect some or all of this bill will become part of Judiciary Committee Chairman Patrick Leahy's (D-VT) proposal, which will almost certainly clear the Judiciary Committee.

As drafted, S.239 would:

- Require that, in the event of a breach companies notify
 - Individuals affected by the breach;
 - Credit reporting agencies if the breach involves the data of more than 1,000 individuals;



- Major media outlets in the relevant jurisdiction and include in that notice the type of data breached and a toll-free number to call for more information, if the breach involves the data of more than 5,000 individuals; and
- The Secret Service if the breach involved the data of more than 10,000 persons.
- Exempt companies from the requirement to notify individuals and the media if an internal risk assessment concludes there is no significant risk of harm and the Secret Service, after reviewing the risk assessment, does not disagree with its conclusion that notice should not be given.
- Preempt conflicting state law.
- Allow for attorneys general to enforce the statute through civil actions.

A copy of the bill is available in the Congressional Record at: <http://www.gpoaccess.gov/crecord/07crpgs.html> (pages S378-S381) and will be available at <http://thomas.loc.gov>.

- **House Oversight and Government Reform Subcommittee to Focus on Data Security** – Following his appointment as chairman of the House Oversight and Government Reform Information Policy Subcommittee, Congressman William Lacy Clay (D-MO) has said he plans to focus the subcommittee on privacy and data security issue. While the subcommittee will primarily focus on the public sector, including follow-up to the data breach at the Department of Veterans Affairs and the government's collection and safeguarding of personal data, Clay has also expressed an interest in looking at how the private sector can better protect sensitive personal information.

III. SPYWARE

- **FTC and Movieland.com Agree to Interim Settlement Pending 2008 Trial** – The U.S. District Court for the Central District of California entered two interim settlements and orders in regards to the FTC's action against Digital Enterprises, Inc. d/b/a Movieland.com. The Commission's August 2006 complaint alleged that the defendants caused software to be downloaded onto consumers' computers that bargaged them with pop-up ads demanding payment to make the pop-ups go away. The pop-up demands represented that someone using the computer consented to the download thereby obligating the computer's owner to pay for it. The software also allegedly altered settings on consumers' computers making the program nearly impossible to remove. Under the settlement, which will remain in effect pending outcome of the trial, the defendants are prohibited from making certain representations regarding the consumers' obligations to pay for the software downloads and must limit the use of pop-up windows. The agreement also requires the defendants to make clear and prominent disclosures when advertising www.movieland.com, www.moviepass.tv, and www.popcorn.net and refrain from installing its software without express consent from consumers.

Links to the August 2006 FTC complaint, the stipulated interim agreements, and press releases regarding each are available at: <http://www.ftc.gov/os/caselist/0623008/index.htm>.



IV. SPAM

- **Failure to Mitigate Not a Limit on CAN-SPAM Penalties** – A District Court ruled that email recipients' efforts to take reasonable steps to block unwanted email does not affect statutory damage claims brought under the CAN-SPAM Act and California's anti-spam provisions. *See Phillips v. Netblue Inc.*, N.D. Cal., No. c-05-4401 (Dec. 12, 2006). The Court concluded that to the extent the damage provisions in both laws are penal, and not compensatory, consideration of mitigation is unwarranted.

Under CAN SPAM, ISPs suing alleged spammers for violations can bring claims for actual or statutory damages. This fact led the court to conclude that statutory damages, in contrast to actual damages, established penal awards. The court also noted judicial discretion in awarding damages, and that the statute's uncapped damage provisions allow for "concerted and willful" conduct, and held that these features were further evidence that Congress intended CAN-SPAM to punish wrongdoers. The court reached a similar conclusion in evaluating the applicable California statutes.

An article announcing, and a copy of, the decision is available at: <http://pubs.bna.com/ip/BNA/EIP.NSF/c7762b49479f833085256b57005afd29/ec21c7caff49d2ae8525725e0076caf?OpenDocument>

- **First Jury Conviction Under CAN-SPAM** – A Californian man, Jeffrey Goodin, who posed as an AOL billing department representative so as to institute a phishing scam, was found guilty last week of sending thousands of fraudulent emails to AOL customers. This outcome represents the first jury conviction under CAN-SPAM. Goodin was also convicted on other counts including wire fraud, aiding and abetting the unauthorized use of credit cards, misuse of the AOL trademark, attempted witness harassment, and failure to appear in court. He will be sentenced in June and faces a maximum sentence of up to 101 years imprisonment.

In effectuating his scam, Goodin used compromised Earthlink accounts to send emails that appeared to originate from AOL's billing department. Recipients were directed to numerous of fraudulent websites where they were instructed to provide personal information or lose Internet access. Once the information was obtained, Goodin, sold it to others or used it himself to make online purchases. Notably, trial testimony revealed that the scam cost Earthlink as much as \$1 million to fight the phishing attack.

An article about this development is available at: http://www.theregister.co.uk/2007/01/17/aol_phishing_fraudster/.

- **Spam Fighting Service Shuts Down** – The Open Relay Database (ORDB), a service aimed at thwarting spammers' attempt to use SMTP proxy servers (or open mail relays) to send junk mail, has closed operations.



Spammers use proxy servers to evade anti-spam filters by incorporating middlemen to send out junk mail. ORDB countered these efforts by distributing blacklists of the implicated servers. The ORDB lists could then be used by administrators to block offending email.

When ORDB opened approximately 90 percent of spam was sent through open relays and now less than 1 percent is sent in this manner. Instead, spammers have, as has been widely reported, turned to botnets to flood email accounts. Consequently, ORDB concluded that their lists were no longer effective in stopping spam.

An article about this development is available at:
<http://uk.news.yahoo.com/22122006/152/plug-pulled-anti-spam-project.html>

- **New Tool Offered to Phishers** – Security experts at RSA have come across a new tool that automatically creates sophisticated phishing sites. The tool is available for \$1,000 on “underground online marketplaces.” As this tool spreads and new phishing sites are created, it will be increasingly difficult for protection technologies to guard against phishing attacks. In particular, because protection software generally uses lists of known phishing sites, and displays a warning to users when those sites are visited, the technology cannot easily protect against brand new sites.

This phishing tool is further evidence of the profitability of phishing sites and is an indication that phishing scams will continue to increase, at least in the immediate future.

An article on this issue is available at: http://news.zdnet.com/2100-1009_22-6149090.html

V. TELECOM/WIRELESS

- **Senator Stevens Introduces New CPNI Legislation** – On January 4, 2007, Senator Stevens (R-AK) introduced S. 92, the “Protecting Consumer Phone Records Act,” which would, among other things, (1) empower a service provider or consumer to bring a private right of action against any person who obtains unauthorized access to that consumer’s Customer Proprietary Network Information (CPNI); (2) require the FCC to enact more stringent regulations to protect CPNI data, including considering applying its rules to providers of IP-based services; (3) specify fine levels of up to \$3 million for continuing violations of CPNI rules; (4) require express consumer consent to include that consumer’s wireless telephone number in a directory assistance service; and (5) provide for concurrent enforcement of its provisions by the FCC, FTC and state authorities. The bill was referred to the Senate Commerce Committee, where it is pending.

A copy of the Protecting Consumer Phone Records Act is available at:
http://thomas.loc.gov/cgi-bin/t2GPO/http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:s92is.txt.pdf



- **Congressman Engel Reintroduces “Truth in Caller ID Act”** – On January 5, 2007, Congressman Engel (D-NY) introduced H.R. 251, the “Truth in Caller ID Act of 2007,” which would make it unlawful to transmit misleading or inaccurate Caller ID information in connection with any telecommunications or VoIP service, and require the FCC to promulgate implementing regulations within six months of enactment. H.R. 251 is virtually identical to H.R. 5126 in the 109th Congress, which passed in the House but did not make it out of the Senate Commerce Committee.

A copy of the bill is available at: http://thomas.loc.gov/cgi-bin/t2GPO/http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h251ih.txt.pdf

- **FCC Fines Phone Data Broker \$97,500 For Failure to Respond to Data Request** – On January 10, 2007, the FCC fined 1st Source Information Specialist, Inc., d/b/a/ LocateCell.com, \$97,500 for the company’s failure to respond to information and document requests relating to the FCC’s investigation of pretexting and other violations of its CPNI rules. The action is further evidence that the FCC has increased its enforcement efforts in connection with CPNI compliance and subscriber privacy. The FCC is expected to issue revisions to its CPNI rules shortly.

Additional information about the FCC’s action in this case is available at:
http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-1A1.doc

- **Legislation to Apply Do-Not-Call Rules to Prerecorded Political Calls Introduced in Congress and Various State Legislatures** – At least three bills have been introduced in Congress that would subject prerecorded political calls to compliance with Federal Do-Not-Call laws.

1. H.R. 248 (the “Robo Calls Off Phones Act,” introduced January 5, 2007, by Congresswoman Foxx (R-NC));
2. H.R. 372 (the “Freedom from Automated Political Calls Act,” introduced January 10, 2007, by Congressman Altmire (D-PA)); and,
3. H.R. 479 (untitled, introduced by Congressman Doolittle (R-CA)).

All three bills would subject politically-oriented recorded message telephone calls to compliance with the FTC’s National Do-Not-Call rules. The principal different between them is that H.R. 248 and H.R. 479 would require implementation by the FTC within 180 days of enactment, whereas H.R. 372 would require implementation within 90 days of enactment.

Bills to extend do-not-call prohibitions to prerecorded political calls also have been introduced or prefiled in Connecticut (SB-157), Florida (SB-322/HB-33), Missouri (SB-49) and Texas (HB-515).



A copy of the H.R. 248 is available at: http://thomas.loc.gov/cgi-bin/t2GPO/http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h248ih.txt.pdf
 A copy of the H.R. 372 is available at: http://thomas.loc.gov/cgi-bin/t2GPO/http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h372ih.txt.pdf
 A copy of the H.R. 479 is available at: http://thomas.loc.gov/cgi-bin/t2GPO/http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h479ih.txt.pdf

Copies of the state bills are available at <http://www.cga.ct.gov/>,
<http://www.capitol.state.tx.us/>, <http://www.myfloridahouse.gov/Sections/Bills/bills.aspx>,
 or <http://www.house.mo.gov/jointsearch/>.

VI. CONSUMER PROTECTION

- **FTC Requests Public Comments on Endorsement Guides** – The FTC announced on January 16, 2007, that it is requesting public comments on the FTC's *Guides Concerning the Use of Testimonials and Endorsements in Advertising*, as part of a systematic review of all its regulations and guides. The FTC is specifically requesting comments about the overall costs, benefits, and regulatory and economic impact of the *Guides*; what effects, if any, changes in technology have had on the *Guides*; two studies commissioned by the FTC on consumer testimonials and any other available research concerning consumer testimonials; and available research on consumers' expectations regarding the compensation of celebrity endorsers. If you are interested in submitting comments to the FTC on any of these issues, please contact one of the Hogan & Hartson attorneys listed below.

The FTC's press release and a link to the text of the Federal Register notice containing information on submitting comments is available at:
<http://www.ftc.gov/opa/2007/01/fyi0707.htm>.

A copy of the FTC's *Guides Concerning the Use of Testimonials and Endorsements in Advertising* is available at: <http://www.ftc.gov/bcp/guides/endorse.htm>.

VII. STATES – ALL ISSUES

- **Additional Data Breach Notification Laws Now in Effect**—As noted in previous *Privacy and Data Security Briefings*, state legislatures have been and will continue to be active in the area of data breach notification and retention. With the new year, several new laws are now in place: Arizona took effect December 31, 2006, Hawaii and Utah on the new year, and Maine's extension of its breach notification law to include all private sector businesses will go into force January 31, 2007. These laws mirror their predecessors in that they focus on unencrypted data that has been or believed to be breached. Michigan's recently passed data breach notification law will go into effect on



July 3, 2007.

In addition, Utah requires data destruction following reasonable business practices if the data is no longer necessary. Several other states will follow this path this year, in passing data destruction laws to complement the data breach notifications laws (33 so far) previously passed.

- **Connecticut Agency Endorses “Children’s Protection Registry Act”** – The Connecticut Department of Consumer Protection released a report whereby they, *sua sponte*, endorsed the establishment of a Children’s Protection Registry Act in Connecticut. As noted in previous *Privacy and Data Security Briefings*, both Utah and Michigan have such Registries, where parents can register “contact points” for their children (email address, IM, cell phone); to the extent a company wants to send a message promoting a product or service that a child is prohibited from purchasing, the company must first check the Registry to determine whether any contact point in their database is registered in either Registry. The costs of checking the Registry is based on the number of contacts in the database, not on the number of contact points identified as part of the search.

The Utah law is being challenged in U.S. District Court, and the law’s premise may have significant constitutional deficiencies. Nonetheless, it is an appealing statement to say, as the Department of Consumer Protection did here, that the Registry is something to consider, at least pending judicial determination of Commerce and First Amendment claims.

An article on the report is available at:
http://www.boston.com/news/local/connecticut/articles/2007/01/14/state_agency_seeks_1_ legislation_establishing_e_mail_registry/.

January 23, 2007 – February 6, 2007.

I. PRIVACY

- **Court Holds Parents Have Right to Privacy in Children’s Names** – The U.S. District Court for the District of Connecticut recently held that parents have a constitutionally protected privacy interest in their children’s names and personal details that would generally prohibit a state from posting such information online. At issue was a Connecticut statute that required the disclosure and publication of top-level state contractors’ dependents. The court found that the Fourth Amendment protects a parent’s privacy interest in a dependent child’s identifying information and that publishing such information on the Internet is not necessary to further the state’s legitimate interests. The court found that more limited distribution or even posting on a password-protected site might be acceptable, but that without any limitations the statute was overly broad. This



case is in contrast with the case discussed in the last *Privacy and Data Security Briefing* in which the District Court for the Southern District of Ohio found that an identity theft victim did not have a federally protected privacy interest in her Social Security number.

A copy of the court's decision in *Securities Industry and Financial Markets Association v. Garfield* is available at: <http://pub.bna.com/eclr/306cv2005.pdf>.

- **Puget Sound Energy Settles Allegations That It Violated Customer Privacy** – Puget Sound Energy (PSE) has agreed to pay a fine of \$900,000 and to contribute \$95,000 to a low-income heating assistance program to settle allegations that it shared customers' information with a third-party marketing company without their written permission, in violation of Washington Utilities and Transportation Commission rules prohibiting such sharing without customers' written permission. In addition to transferring basic customer information, PSE allegedly transferred 65,000 calls over five years to a marketing company that then marketed household services to PSE's customers. The \$95,000 is the estimated amount of revenues PSE obtained through its unlawful transfer of customers' information.

An article on this issue is available at:
http://seattletimes.nwsourc.com/html/localnews/2003536577_webpse22.html

A government press release on this issue is available at:
<http://www.wutc.wa.gov/webimage.nsf/0/BF76A2EF38C0185B8825726B00760457>

- **Zogby Poll Looks at Privacy Expectations** – In a recent Zogby International Survey on behalf of the Congressional Internet Caucus Advisory Committee, 91% of respondents agreed with the statement that expectations of privacy have changed due to technologies and the Internet. Respondents ages 18 to 24 were less likely than others surveyed to believe that activities such as someone posting a picture of them in a swimsuit constituted an invasion of their privacy.

An article on this issue is available at:
<http://www.govtech.net/news/news.php?id=103678>

II. SECURITY

- **Congressman Frank Plans to Introduce Data Breach Notification Legislation** – House Financial Services Committee Chairman Barney Frank (D-MA) says he plans to introduce data breach notification legislation this year. Perhaps hoping to head off the stalemate that occurred last year between his committee and the House Energy and Commerce Committee, Frank said he would work with Commerce Committee Chairman John Dingell (D-MI) to draft consensus legislation. Frank has been a regular critic of retailers' failure to notify banks immediately of a breach of credit card data, since many state laws allow for such delay for law enforcement purposes. Frank has said he would like to force merchants to disclose breaches immediately to card issuers to help prevent



fraud, and any legislation he introduces will likely include such a requirement. Frank has also said he supports a notification exemption when the data is encrypted.

More information on this issue is available at: http://www.washingtonpost.com/wp-dyn/content/article/2007/02/01/AR2007020100748_pf.html

- **Retailer Faces Class Action Lawsuit Over Data Breach** – TJX Co., the parent-company of T.J. Maxx and Marshalls, has been sued in U.S. District Court in Boston following a breach of credit card data. The suit seeks credit monitoring services and any damages caused by the breach. The breach occurred in May of 2006 and TJX discovered it in December but delayed publicly announcing it for a month. After considering offering credit monitoring services to affected customers, the company decided against doing so, telling consumers that the stolen information is unlikely to be used for identity theft. This decision has been criticized by consumer advocates, and at least one IT security vendor, particularly since the breach was the result of a hacking attack.

While TJX has not announced how many customers were affected, the Massachusetts Bankers Association (MBA) has said that member banks have reissued hundreds of thousands of debit and credit cards and that it has received reports of fraudulent charges. MBA also reported that the lost data included card numbers, names, and in some cases, encrypted PINs. Payment Card Industry Standards prohibit maintaining PIN information.

In addition to the pending class action suit, Amerifirst Bank of Alabama has filed a suit seeking to recover the cost of replacing customers debit cards, and Congressman Edward Markey (D-MA) has called on the FTC to launch an investigation of the breach.

More information on the issue is available at:
http://www.boston.com/business/articles/2007/01/30/tjx_faces_class_action_lawsuit_in_data_breach/

III. SPYWARE

- **Sony BMG Settles FTC Charges Alleging Anti-Piracy/Spyware** – Sony BMG Music Entertainment (Sony BMG) settled FTC charges brought under Section 5(a) of the FTC Act that resulted from Sony BMG's use of Digital Rights Management software embedded in its CDs in part to prevent illegal reproduction. The FTC claimed that Sony BMG acted unfairly when it allegedly caused software to be installed on consumers' computers that created a security risk and failed to provide reasonable means to locate or remove it. In addition, the FTC claimed that Sony BMG acted deceptively when it failed to disclose that software would be installed on consumers' computers that (1) limited consumers' ability to play and copy the CD; and (2) monitored and reported consumers' listening preferences in order to serve targeted marketing messages.

Under the settlement, Sony BMG is barred from using any information about consumer listening preferences that it has already acquired. Sony BMG is also precluded from



selling CDs containing content protection software that prevents consumers from finding or removing that software and that does not contain an easy and reasonable method to remove it. Sony BMG must also exchange any CDs containing concealed software with replacements, and reimburse some consumers up to \$150 for damage incurred attempting to remove the software. The settlement also requires Sony BGM to:

- o provide adequate disclosure and obtain consumer authorization before content protection software is installed on a consumer's computer in the future;
- o include clear and prominent disclosure of copying or use restrictions on the packaging of CDs; and
- o disclose on the packaging any requirements to install software that monitors consumers' music preferences and obtain consumer authorization before the software sends information back to Sony BMG.

The FTC joins Texas and California who settled similar charges in December 2006 (*see* Dec. 18, 2006 *Privacy and Data Security Briefing*).

The FTC press release regarding the settlement is available at: <http://ftc.gov/opa/2007/01/sony.htm>

The Complaint, Consent Order, and Analysis regarding *In re Sony BMG Music Entertainment*, is available at: <http://ftc.gov/os/caselist/0623019/index.htm>

- **Anti-Spyware Coalition Releases Best Practices Recommendations** – On January 25, 2007, the Anti-Spyware Coalition released two reports: *Best Practices: Factors for Use in the Evaluation of Potentially Unwanted Technologies* and *Conflict Identification and Resolution Process*. The *Best Practices* report is intended to help anti-spyware vendors identify technological behaviors that are cause for concern, as well as those that limit the negative impact of potentially unwanted technologies. The *Conflict Identification and Resolution Process* suggests ways in which anti-spyware tools that conflict with one another can be resolved. The Anti-Spyware Coalition is hopeful that the two documents will help software developers avoid publishing software that is unwanted by consumers. Both documents are posted on the group's website and public comment is welcome.

A copy of the Anti-Spyware Coalition's *Best Practices* document is available at: <http://www.antispywarecoalition.org/documents/BestPractices.htm>

A copy of the Anti-Spyware Coalition's *Conflict Identification and Resolution* document is available at: <http://www.antispywarecoalition.org/documents/ConflictsResolution.htm>

IV. SPAM

- **FTC Announces Settlement Under CAN-SPAM** – The FTC and the Department of Justice (DOJ) have reached a settlement with TJ Web Productions, LLC, ("TJ Web"), an adult entertainment Internet marketer, in connection with charges that the company



initiated sexually explicit commercial emails in violation of applicable laws and regulations.

Under CAN-SPAM and the FTC's Adult Labeling Rule, commercial emailers of sexually explicit material must include the phrase "SEXUALLY EXPLICIT:" in the subject line, and ensure that the initially viewable area of the message does not contain graphic sexual images. In addition, unsolicited commercial email must include an opt-out mechanism and a postal address. TJ Web is charged with violating these provisions through an "affiliate marketing" program in which it induced others, by monetary payments and other consideration, to transmit commercial email messages on its behalf.

Under the proposed settlement, TJ Web is permanently prohibited from violating the FTC's Adult Labeling Rule and from initiating commercial email without clearly and conspicuously displaying a physical postal address and a functioning opt-out mechanism. The proposed settlement also requires TJ Web Productions to obtain agreement from prospective affiliates to comply with the terms of the court order, and to inform them that any violations will lead to immediate termination from its affiliate program and forfeiture of payments.

The FTC initially filed its complaint against TJ Web in July 2005 in connection with an effort to combat illegal "X-rated" commercial emails. Six other companies were also charged with violating federal laws requiring warning labels on sexually explicit email. FTC has already reached settlements with five of these companies resulting in civil penalties totaling \$1.624 million. Under the latest settlement, TJ Web will pay a \$465,000 civil penalty.

While the charges under the Adult Labeling Rule are more relevant to companies operating in that space, the allegations relating to the opt-out mechanism and postal address are increasingly common in FTC causes of action brought under CAN-SPAM. All companies are encouraged to continually monitor their commercial emails to ensure that they are complying with CAN-SPAM.

The FTC's Press release and related documents are available at available at: <http://www.ftc.gov/opa/2007/01/tjweb.htm>

- **MySpace Files Complaint Against "Spam King"** – Social-networking site MySpace has filed suit in a U.S. District Court in Los Angeles against notorious spammer Scott Richter after Richter allegedly sent millions of unsolicited "bulletins" to MySpace users' accounts. The bulletins were allegedly sent between July 2006 and December 2006 in violation state and federal laws, including California's anti-spam statute and the CAN-SPAM Act. MySpace maintains that Richter either phished MySpace accounts himself or acquired a list of phished accounts from a third party. In the complaint, MySpace seeks a permanent injunction barring Richter and his affiliated companies from MySpace, and punitive damages totaling at least \$50 per spam message sent.



Notably, Richter has already paid several million dollars in connection with lawsuits brought by the New York Attorney General and Microsoft but had maintained in public statements that he is now focused on legitimate operations. Consumer activists have been skeptical of Richter's claims.

An article about this development is available at:
http://www.esecurityplanet.com/best_practices/article.php/3655991

- **Attorneys Fees Not Awarded Absent Bad Intent** – A U.S. District Court in the Northern District of California will not award attorneys' fees to a successful defendant in a CAN-SPAM case absent a showing of bad intent or frivolousness on the plaintiff's part. See *Phillips v. Worldwide Internet Solutions Inc., N.D. Cal., No. C 05-5125, 1/22/07*.

CAN-SPAM section 7706(g)(4) authorizes the courts to use their discretion to "assess reasonable costs, including reasonable attorneys' fees, against any party." Consequently, Defendant Worldwide Internet Solutions, after defeating a plaintiff's CAN-SPAM claims on jurisdictional grounds, sought attorneys' fees. In response, the plaintiff maintained that attorneys' fees should be awarded only if the claims are "frivolous, unreasonable, or groundless." The defendant challenged that CAN-SPAM did not include statutory language requiring frivolousness in an award of fees.

Ultimately, the magistrate, finding neither unreasonableness or frivolousness on the plaintiff's part (and noting that the merits plaintiff's claims had not been evaluated) concluded that an award of attorneys' fees on these facts would violate congressional intent because such an award would likely deter the future litigation of legitimate harms for fear of penalty.

An article about the decision is available at:
<http://pubs.bna.com/ip/BNA/EIP.NSF/7c407ecc8216ce4185256d05005e8b30/029c8a7382e9234e8525727400062bc6?OpenDocument>

The full text of the opinion is available at: <http://pub.bna.com/eclr/4055125.pdf>

- **Regions Bank Falls Victim to Phishing Scam** – Regions Bank is the latest financial institution used in a phishing scam. Like other similar scams perpetrated on the customers of financial institutions, emails using the Regions Bank logo asks recipients to renew online accounts and subsequently directs customers to a fraudulent site where their information is collected. The fraudulent emails contain some clues as to their illegitimacy in that the communication includes misspelled words and bad grammar.

The latest scam comes in the wake of recent reports asserting that phishing scams are on the rise and now outnumber Trojans and other viruses. Security mail services vendor MessageLabs has just reported that in January 2007, one in 93.3 (1.07%) emails involved



a phishing attack with only one in 119.9 emails (0.83 percent) resulting from virus attacks.

An article about Regions Bank phishing attack is available at:
<http://www.al.com/business/mobileregister/index.ssf?/base/business/1169547788286420.xml&col=3>

An article about the rise in phishing scams is available at:
<http://news.zdnet.co.uk/security/0,1000000189,39285691,00.htm>

V. TELECOM/WIRELESS

- **NJ Assembly Passes Bill Prohibiting Unsolicited Text Messages** – On January 29, 2007, the New Jersey Assembly passed AB-3231, which, if enacted, would prohibit the transmission of commercial text messages to wireless devices absent the prior express permission of the message recipient. The bill does not define "prior express consent" but it appears that a signed writing would not be required because language to the effect was removed from the bill prior to passage. The prohibition would apply to any commercial text message intended to encourage a purchase, rental, or investment, and for which the recipient would incur a charge or usage allocation deduction. Attention now is expected to turn to the State Senate, which is considering S-1130, an identical measure.

Additional information about AB-3231 and S.1130 can be found at:
<http://www.njleg.state.nj.us/bills/BillView.asp>

- **"Voice Broadcaster" Settles FTC Investigation With \$1 Million Fine** – The FTC announced on February 2, 2007, that a "voice broadcaster" (*i.e.*, an entity responsible for the mass transmission of autodialed prerecorded calls) has agreed to pay a \$1 million fine to resolve multiple violations of the FTC's Telephone Sales Rule ("TSR"). According to the announcement, a Florida-based entity called "The Broadcast Team" transmitted over 64 million calls to consumers in violation of the TSR. Of particular note is the FTC's determination that The Broadcast Team's practice of calling consumers and hanging up on live voice responses violated the TSR's call abandonment rules.

Additional information about the FTC's action can be obtained at:
<http://www.ftc.gov/opa/2007/02/broadcastteam.htm>

- **Additional "Anti-Spoofing" Measure Introduced in Congress** – On January 31, 2007, Congressman Scott (D-VA) introduced H.R. 740, the "Preventing Harassment through Outbound Number Enforcement (PHONE) Act of 2007," which would prohibit the transmission of false Caller ID information with the intent to deceive the call recipient, a practice commonly referred to as "spoofing." The Act would punish violators with fines or potential prison terms of up to five years, as well as through forfeitures. Law enforcement agencies would be exempt from the Act, but it would apply to all types of



phone service, including VoIP service. The House Committee on Crime, Terrorism and Homeland Security considered the Act at a hearing on February 6, 2007.

Additional information about H.R. 740, including the text of the legislation can be found at: <http://thomas.loc.gov/cgi-bin/thomas>

VI. GRAMM-LEACH-BLILEY ACT

- **Third Circuit Rules on Applicability of Gramm-Leach-Bliley (GLB)** – The Third Circuit, in *Chao v. Community Trust Company, Nos. 05-2785/4828, 1/19/2007*, overruled a district court and found that (1) GLB applies to employee benefit trusts; and (2) government agencies cannot subpoena information protected by GLB without first making a showing that the agency has jurisdiction.

The first ruling, while limited in scope, is important in that it broadly defines a consumer to include employee benefit trusts, despite an FTC rulemaking that declares “an individual is not your consumer solely because he or she is a participant or beneficiary of an employee benefit plan that you sponsor or for which you act as a trustee or fiduciary.” In making this ruling, the court declined to give the FTC’s regulatory interpretation deference in an action involving the Department of Labor (DOL).

The second ruling is more significant for companies defending a subpoena under GLB. GLB allows companies to disclose information to third parties without notice and consumer consent when the disclosure is pursuant to a “properly authorized . . . subpoena.” DOL argued that the information it sought was necessary to determine its jurisdiction. The Third Circuit rejected this argument holding that a “properly authorized” subpoena requires the existence of jurisdiction to undertake the investigation. The court also found that a determination of jurisdiction was possible without disclosing consumers’ non-public information. In concluding that GLB barred enforcement of the subpoena, the court said that “in order to make [GLBs] protections meaningful, before private consumer financial information is released by a financial institution to the DOL, the Secretary must establish jurisdiction to conduct the investigation.”

The court also held that the Right to Financial Privacy Act did not bar enforcement of the subpoena.

A copy of the decision is available at:
<http://www.ca3.uscourts.gov/opinarch/052785p.pdf>

VII. CONSUMER PROTECTION

- **Court Finds Allegedly “Free” Software Is Deceptive** – A magistrate judge for the U.S. District Court for the Eastern District of Texas held that hidden fees and buried terms in connection with software advertised as “free” were deceptive in violation of Section 5 of the FTC Act. The company advertised its software as free, but its terms of agreement



contained language stating that the “bonus” CDs the customer would receive had to be returned within 10 days or the customer would incur charges. The court found that the material terms regarding the charges and the 10-day period were not adequately disclosed and were therefore deceptive.

The FTC also held a workshop on negative option marketing on January 25, 2007. This case and the workshop may reflect a heightened interest in and awareness of this type of marketing.

The FTC’s press release and related documents are available at:
<http://www.ftc.gov/opa/2007/01/manay.htm>

VIII. STATE LEGISLATIVE AND ENFORCEMENT ACTIVITIES

- **New York Attorney General settles with advertisers who used purported spyware --** The New York attorney general reached settlements with three well-known companies relating to their online ad delivery through third party software programs. The companies were charged with online promotion of products and services through another company’s (Direct Revenue) alleged deceptively installed adware programs. The conclusion of this case represents the first time in which advertisers were held responsible for ads displayed through downloadable adware programs, and potentially ushers in a new law enforcement era of bringing deception claims against parties beyond the primary perpetrators of the acts.

The Attorney General’s press release is available at:
http://www.oag.state.ny.us/press/2007/jan/jan29b_07.html

A Hogan & Hartson *Privacy Update* on the issue is available at:
<http://www.hhlaw.com/newsstand/pubDetail.aspx?publication=2844>

- **States beginning to balk at costs associated with REAL ID Act** – When the REAL ID Act was passed in May 2005, it was heralded as a necessary step in the fight against terrorism, and would create a national’s driver’s license data-sharing program. REAL ID provides that if state identity cards are to be acceptable for federal purposes, such as airline passenger screening by Transportation Security Administration officials, the state cards, such as driver’s licenses, must be machine readable and tamper resistant. At this point, the DHS implementing provision has not yet been introduced, and it is quite likely that the May 2008 deadline for compliance is in jeopardy. As a result of the DHS delay, concern by state administrators about the costs and privacy implications has increased discussions on state obligations in several legislatures. In 2007, at least Vermont, Georgia, Washington, Montana, and Maine have introduced legislation challenging the imposition of the REAL ID Act; on the other side, lawmakers in California, Maryland, Missouri, New Jersey and Oregon have introduced bills that would conform state practices and procedures to comply with the federal law. Nationwide compliance on



REAL ID by May 2008 is going to be difficult, particularly with the state dissention and delay.

- **Maryland, six other states introduce a data breach notification bill** – Maryland, now in the minority of states without a data breach notification law, introduced one last week in the legislature. The "Personal Information Protection Act," sponsored by Del. Tanya Thornton Shewell (R), applies to both hard copy and electronic data, even if it is encrypted. The definition of personal information mirrors most state laws, and includes first and last name plus, among others, Social Security number, Driver's license, or account information plus an access code. Six other states--Alaska, Massachusetts, Oregon, South Carolina, Virginia, and Wyoming—are also considering new data breach notice bills during their 2007 legislative sessions.

Maryland's bill as introduced is available at:
<http://mlis.state.md.us/2007RS/bills/hb/hb0090f.pdf>

- **New Jersey Court finds privacy right to subscriber information** – In a decision that is inconsistent with most holdings relating to subpoenas for Internet subscriber records, a New Jersey court in *New Jersey v. Reid*, N.J. Super. Ct., App. Div., has held that a subscriber has privacy right to her records with her ISP. This decision is grounded in the New Jersey Constitution, which has an express right to privacy, as opposed to the federal Constitution. A police officer sought ISP records relating to a computer crime; the ISP provided the information, and the subscriber sued, claiming that her reasonable expectation of privacy had been violated. This decision could reek havoc with ordinary law enforcement mechanisms in New Jersey, and could provide a safe harbor for criminal activities.

The decision is available at: <http://pub.bna.com/eclr/nja342405.doc>

IX. INTERNATIONAL ACTIVITIES

Canada – Bank's Disposal of Customer Financial Information Violated PIPEDA – A major Canadian bank violated Canada's federal privacy law, the Personal Information Protection and Electronics Documents Act (PIPEDA), by improperly disposing documents that contained customer financial information. The customer's personal and investment information, including name, address, social insurance number, account number and transaction history, was discovered in an unattended recycling bin in an underground parking garage. The customer filed a complaint with the Office of the Privacy Commissioner of Canada. The Assistant Commissioner determined that the bank did not have effective measures in place to ensure that the complainant's personal information was adequately protected from unauthorized disclosure, in violation of PIPEDA Principles 4.7 and 4.7.5. As a result, the bank was required to develop a policy to ensure that when an employee leaves the bank, there is a systematic approach to securing any confidential client information in that employee's custody. After the bank confirmed having such a process, and indicating that certain lines of business may have



additional customized processes that align with their specific business, and that an enhanced and more comprehensive protocol for departing employees is under development, the Assistant Commissioner was satisfied that the bank had met its obligations. The Commissioner's Office released its opinion on January 24, 2007, though it had issued its ruling in October 2006.

For the full text of PIPEDA Case Summary #356, see: http://www.privcom.gc.ca/cf-dc/2006/356_20061023_e.asp

X. RADIO FREQUENCY IDENTIFICATION TECHNOLOGIES (RFID)

- **Smart Card Alliance Issues Best Practices for RF-Enabled Technology in Identity Management** – On January 29, 2007, the Smart Card Alliance (Alliance) issued best practice suggestions for entities that utilize radio frequency (RF) technology in identity management systems. The best practice suggestions include a set of three guidelines for security and a set of seven guidelines for personal privacy protection. According to the Alliance, the recommended guidelines will help to "ensure the confidentiality, integrity and validity of identity information and protect the credential holder's privacy." In addition to issuing the best practices, the Alliance also issued frequently asked questions (FAQs). The FAQs provide additional detail regarding the best practices, as well as seek to clarify a common misconception that RF-enabled technologies used to transmit identity information are the same as radio frequency identification (RFID) technologies used in manufacturing, shipping, and object-related tracking. One difference noted by the Alliance is that RF-enabled technologies are able to satisfy the Alliance's best practice suggestions, whereas RFID technologies have minimal built-in support for security and privacy.

A copy of the Alliance Best Practices and FAQs is available at:
<http://www.smartcardalliance.org/pages/publications-rf-technology-best-practices>

A copy of the Alliance Press Release is available at:
<http://www.smartcardalliance.org/articles/2007/01/29/smart-card-alliance-recommends-best-practices-for-use-of-rf-technology-in-identity-management>

An article on this issue is available at:
<http://www.eweek.com/article2/0,1759,2088544,00.asp?kc=EWRSS03119TX1K000594>

- **Technology Trade Groups Establish RFID Council** – The American Electronics Association, AIM Global, European-American Business Council, IEEE-USA, the Information Technology Association of America, the Information Technology Council, the International RFID Business Association, and the Semiconductor Industry Association have formed an ad-hoc group called the RFID Technology Council. In addition to supporting the use of RFID technologies, the Council will support the U.S. Senate RFID Caucus, which is co-chaired by Senators Byron Dorgan (D-ND), and John



Comryn (R-TX). The Senate RFID Caucus formed in mid-2006 to explore the benefits and policy challenges associated with RFID technologies, including privacy and security concerns, the role of RFID in national security and industrial applications, and the need for standards and interoperability.

An article reporting on the formation of the RFID Technology Council can be found at: http://www.cio-today.com/news/Tech-Trade-Groups-Form-RFID-Council/story.xhtml?story_id=113007H79EHQ

An article regarding the Senate RFID Caucus can be found at: <http://www.rfidjournal.com/article/view/2452>

February 7, 2007 – February 20, 2007.

I. PRIVACY

- **Data Retention Legislation Introduced** – Representative Lamar Smith (R-TX), ranking minority member of the House Judiciary Committee, has introduced a data retention measure as part of the broader SAFETY Act. The provision is quite open-ended and leaves the details to the Attorney General, requiring the Attorney General to issue regulations governing the retention of records by Internet Service Providers. The regulations shall require the retention of data such as the name and address of the subscriber or registered user to whom an IP address or telephone number was assigned. Anyone who knowingly fails to retain a required record will face fines and/or imprisonment of up to one year. Otherwise, the provision leaves the details entirely up to the Attorney General.

Privacy advocates and industry members have expressed concern over the vagueness of the bill and have raised a number of potential issues. The legislation does not limit what data would be required to be retained or for how long, leaving open the possibility that Internet Service Providers could be required to retain the full content of emails and instant messages for long periods of time (or forever). The definitions of affected parties are vague (and contradictory), therefore, the draft legislation does not make clear what types of providers would be affected; furthermore, it is unclear whether government entities, schools, libraries, and/or wi-fi providers would be covered. The legislation as written could allow private litigants in civil cases to obtain the retained records. The massive storage requirements and the potential for data breach or misuse have also been raised as downfalls of the legislation.

This data retention provision is much broader than the proposal drafted last year—and discussed in previous issues of the *Privacy and Data Security Briefing*—by Representative Diana DeGette (D-CO). Attorney General Alberto Gonzales has been advocating mandatory data retention requirements for about a year as essential to the



fight against child pornography. We will continue to monitor the progress of this bill as well as the opposition against it.

Articles on this issue are available at: http://news.com.com/2100-1028_3-6156948.html and <http://www.washingtonpost.com/wp-dyn/content/article/2007/02/12/AR2007021201337.html>.

A copy of the draft SAFETY bill is available at: <http://www.politechbot.com/docs/smith.data.retention.labeling.draft.020607.pdf>.

- **Company Can Give Third-Party Consent to Search Employee's Office Computer** – The U.S. Court of Appeals for the Ninth Circuit recently decided that the Fourth Amendment rights of a company executive were not violated when the company's CFO gave an FBI agent a copy of the defendant's hard drive (taken from the defendant's locked office) at the request of an FBI agent who had received a tip from the company regarding child pornography. The Ninth Circuit looked at whether an employee has an expectation of privacy in his workplace computer sufficient to suppress evidence of child pornography in a criminal prosecution. Initially, in August 2006, the Court found that private employees did not have a reasonable expectation of privacy, and thus no Fourth Amendment rights, in their workplace computers. *See U.S. v. Ziegler*, 456 F.3d 1138 (9th Cir. 2006). However, upon a petition for a rehearing, the Ninth Circuit changed its initial ruling and issued a new opinion concluding that the employee had a reasonable expectation of privacy in the locked office where his computer was located but that the lower court could admit the evidence of pornography, because the employer had the right to consent to the government's search.

Courts across the country have reached different results on the issue of employees' reasonable expectations of privacy in workplace computers, especially in the face of company policies stating that the computers are subject to monitoring. The Ninth Circuit avoided that question somewhat by focusing on the locked office and determining that the employer was able to provide third-party consent and fall within an exception the Fourth Amendment's warrant requirement.

The Ninth Circuit's decision is available at: [http://www.ca9.uscourts.gov/ca9/newopinions.nsf/1B9EE38656401781882572720080706B/\\$file/0530177.pdf?openelement](http://www.ca9.uscourts.gov/ca9/newopinions.nsf/1B9EE38656401781882572720080706B/$file/0530177.pdf?openelement).

II. SECURITY

- **Senators Leahy and Specter Introduce Data Security Bill** – On February 6, Senate Judiciary Committee Chairman Patrick Leahy (D-VT) and Ranking Member Arlen Specter (R-PA) introduced S.495, which closely tracks legislation the pair introduced last Congress. S.495, the Personal Data Privacy and Security Act of 2007, includes the following provisions:



- Enhanced Criminal Penalties: The law would create new criminal penalties for identity theft and concealing a data breach.
- Data Broker Requirements: The law would require data brokers to provide consumers with all of their electronic records at their request and for a reasonable fee. Data brokers would also be required to establish a detailed accuracy resolution process. Violations would be punishable by up to \$1,000 per violation in civil fines. These requirements would not be imposed on data brokers in compliance with Gramm Leach Bliley (GLB) or the Health Insurance Portability and Accountability Act (HIPAA) or on products provided in compliance with the Fair Credit Reporting Act (FCRA).
- Data Privacy and Security Program: The law would require all business entities to establish a data privacy and security program. While this requirement is modeled on the data security requirements in GLB, it is much more detailed. Moreover, the bill would only exempt companies covered by GLB if they are also subject to examinations by federal banking or insurance regulators. HIPAA covered entities are also exempt. All other companies would be required within one year of passage of the bill to develop a plan that would require them to:
 - Perform a risk assessment to identify potential vulnerabilities.
 - Develop of privacy and data security program that addresses administrative, technical, and physical aspects identified by the Federal Trade Commission (FTC) in rulemaking.
 - Train employees on the implementation of the privacy and data security program.
 - Conduct “regular testing” of the privacy and data security program.
 - Contractually ensure that service providers that handle sensitive data implement similar safeguards.
 - Periodically review the privacy and data security program and update it as necessary.
 - Violations would be subject to a \$5,000 fine per violation for a maximum fine of \$500,000 and injunctive relief as enforced by the FTC.
 - This section broadly preempts state law, but state attorneys general are empowered to enforce these requirements in federal court. No private cause of action is available.
- Date Breach Notification: The law would require notice to individuals, law enforcement, and the media in the event of a data breach.
 - Notice to affected individuals is required for all breaches and major media outlets must also be notified when the breach affects more than 5,000 people. The notice may be delayed to ensure the breach is contained. Law enforcement must also be notified in certain circumstances.
 - The bill does not contain a specific exemption for encrypted data, but does allow companies to conduct a risk assessment and show that there is “no significant risk” of harm to individuals. This assessment must be



- submitted to the U.S. Secret Service within 45 days of discovery of the breach. The Secret Service then has 10 days to challenge the assessment and require notice.
 - Businesses that employ financial fraud protection protocols that prevent fraudulent transaction have a limited exemption to the notice requirement.
 - Significantly, S.495 expands on the list of information most states use to require a breach notification. Most states followed California’s lead and required notification if the breach involved names plus either a Social Security number, driver’s license number, account number, or credit/debit card number plus PIN. To this list, S.495 adds:
 - Any two of the following:
 - Home address or telephone number
 - Mother’s maiden name
 - Month, day, and year of birth
 - A unique biometric identifier, such as a finger print.
 - A unique account identifier or user name in combination with any required password.
 - Violations of the law would be punishable by a fine of \$1,000 per day per person for a maximum of \$1,000,000 and would be enforced by the Department of Justice.
 - State law requiring breach notifications would be preempted, but state attorneys general would be able to bring claims. There would be no private right of action.
- Government Use of Commercial Data: The law would require a series of audits to assess how the government uses commercial data and employs private sector companies to handle personally identifiable information.

As reported in the January 29, 2007 *Privacy and Data Security Briefing*, Senator Diane Feinstein (D-CA) introduced S.239, the Notification of Risk to Personal Data Act, which will also be considered by the Judiciary Committee. Last Congress, Senator Feinstein introduced a similar bill, portions of which were incorporated into the bill that eventually passed out of the Judiciary Committee. We expect that a similar outcome is likely this year and that S.495 has an excellent chance of being approved by the Judiciary Committee. The key issue will be whether differences with other Committees that may pass competing legislation can be resolved.

Senate Majority Leader Harry Reid (D-NV) issued a press release supporting S.495 and said that passing data security legislation is a priority, improving the chance the bill will pass the full Senate.

A copy of the bill is available at: http://thomas.loc.gov/cgi-bin/t2GPO/http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:s495is.txt.pdf.



- **Congressmen Rush and Stearns Introduce Data Security Bill** – House Commerce Subcommittee on Commerce, Trade and Consumer Protection Chair Bobby Rush (D-IL) and ranking member Cliff Stearns (R-FL) have reintroduced the Data Accountability and Trust Act. The bill contains the following provisions.
 - **Data Security Plan:** The law would require companies to implement a set of information security practices. The requirements for these security practices are closely modeled after GLB, but also include a requirement that they incorporate a process for properly disposing of paper and electronic records. The FTC is authorized to exempt companies that are in compliance with other federal laws requiring data security standards.
 - **Proper Disposal of Sensitive Data:** The law would require the FTC to conduct a study on the practicality of requiring a standard method for the destruction of data and would authorize the FTC to implement regulations to enforce a standard method of destruction.
 - **Requirements for Data Brokers:** The law would require information brokers to establish reasonable procedures to verify the accuracy of information they collect, give individuals free access to their information once per year, and establish a process for correcting inaccurate information. In the event of a data breach, data brokers would be required to submit their security policies to the FTC and undergo an FTC audit. Finally, information brokers would be prohibited from pretexting or gaining information by false pretenses. The FTC may exempt entities defined as “consumer reporting agencies” under the FCRA from compliance with this section.
 - **Data Breach Notification:** In the event of a data breach, the law would require companies to notify the FTC and any individual affected by the breach.
 - The trigger for breach notification tracks the California standards and does not include the additional categories contained in S.495 discussed above.
 - Substitute notice procedures are available if the company has records on less than 1,000 people and direct notification is not feasible.
 - Companies would also be required to provide free credit monitoring for two years, upon request, to any consumer affected by the breach.
 - The law would exempt companies from this requirement if the data is encrypted.
 - The law would be enforced by the FTC and by state attorneys general. Civil penalties for failure to have a data security plan would be \$11,000 per day with a maximum penalty of \$5,000,000. Civil penalties for failure to notify individuals of a data breach would be \$11,000 per person with a maximum penalty of \$5,000,000.



- **Preemption:** The law would preempt state laws requiring data security plans or data breach notification.

This bill passed the Commerce Committee last year as H.R. 4127 and will almost certainly clear the Committee again. The bill never made it to the House floor following a stalemate with the House Financial Services Committee, which had passed competing legislation. Such deadlock is possible again this year, although Commerce Committee Chairman John Dingell (D-MI) and Financial Services Committee Chairman Barney Frank (D-MA) have pledged to find common ground.

A copy of the bill is available at:
http://energycommerce.house.gov/privacy/HR_computer_data.pdf.

- **Congressman Markey Introduces Bill to Restrict the Use of Social Security Numbers** – Congressman Edward Markey (D-MA) introduced H.R. 948, the Social Security Number Protection Act, which would restrict the sale or purchase of Social Security numbers. The specific restrictions are left to the FTC to determine in rulemaking, but exemptions would be made for sale or purchase with the consumer’s consent or for credit verification purposes. The law would be enforced by the FTC and state Attorneys General. State laws restricting the sale or purchase of Social Security numbers would be preempted.

A copy of the bill is available at: http://thomas.loc.gov/cgi-bin/t2GPO/http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h948ih.txt.pdf.

III. SPYWARE

- **SPY ACT Reintroduced in the House** – Representatives Edolphus Towns (D-NY) and Mary Bono (R-CA) reintroduced the Securely Protect Yourself Against Cyber Trespass Act (SPY ACT) on February 8, 2007. The legislation (H.R. 964) is nearly identical to legislation of the same name passed in the 108th and 109th Congresses, both of which failed to gain Senate approval. Like its predecessors, H.R. 964 aims to protect consumers from several unfair and deceptive acts in connection with specified conduct including modifying computer settings, collecting personally identifiable information, and removing or disabling security or anti-spyware technology. Specifically, the Act would prohibit the transmission of any information collection program to a user’s computer unless that program provides adequate notice, as specified in the Act, before execution of the program’s collection functions. The Act would also prohibit the execution of an information collection program installed on a computer unless the user consents to the execution of the collection function after receiving adequate notice, as specified by the Act.

The Act includes a “Good Samaritan” provision which exempts software and service providers taking action in good faith and with users’ consent. The Act would also



preempt state spyware laws and would prohibit private rights of action based on violation of the Act.

The SPY ACT has been referred to the House Committee on Energy and Commerce where the Committee's chairman, Congressman John Dingell (D-MI), promises to pass it on to the House "expeditiously." We will continue to monitor the progress of the SPY ACT and related legislation through the legislative process.

The full text of H.R. 964 is available at:

http://thomas.loc.gov/home/gpoxmlc110/h964_ih.xml.

- **DirectRevenue Settles FTC Charges** – The Federal Trade Commission announced on Friday, February 16, 2007, that it had settled charges against DirectRevenue LLC and its affiliates regarding the company's development, marketing, and distribution of adware. The Commission's complaint alleges that DirectRevenue bundled adware that subsequently delivered targeted pop-up advertising, with other content such as screensavers, games, and utility programs. The complaint also alleges that in many cases, consumers were unaware that the adware would be installed on their computers, because notice was inadequate or nonexistent, and that the respondents made identifying and removing the adware extremely difficult.

The Commission's complaint alleges that bundling the adware with the desired utilities, screensavers, and other desired software without adequate notice or consent was a deceptive practice in violation of Section 5 of the FTC Act. The installation of adware that could not be identified or easily removed was an unfair practice according to the Commission.

Terms of the settlement include:

- o Prohibiting respondents from serving any ads to computers on which respondents' software was installed prior to October 1, 2005;
- o Prohibiting respondents from installing or assisting other in the installation of any software that exploits security vulnerabilities or installs an application without consumers' express consent;
- o Requiring respondents to establish and implement a program designed to require affiliates to obtain express consent before installing respondent's software;
- o Requiring respondents to identify advertisements served by its software so that consumers can easily locate the source of those advertisements;
- o Requiring respondents to provide to consumers effective means to uninstall the adware; and
- o Requiring respondents to disgorge \$1.5 million in ill-gotten gains.



Commissioner Leibowitz issued a dissenting statement supporting the injunctive relief obtained by Commission staff while stating that the \$1.5 million monetary relief was insufficient.

The FTC press release regarding the settlement is available at: <http://www.ftc.gov/opa/2007/02/directrevenue.htm>.

The Complaint, Consent Order, Analysis, and Commissioner Leibowitz's Dissent regarding *In re DirectRevenue LLC*, is available at: <http://www.ftc.gov/os/caselist/0523131/index.htm>.

IV. SPAM

- **Class Action Settlement Approved in Case Challenging Cell Phone Spam** – The spread of spam to cell phones (also known as spim) has garnered increased attention, and the courts are now getting involved. A District Court Judge for the Northern District of Illinois has reached a preliminary ruling in favor of a class action plan that would provide up to \$150 each for approximately 1,000 consumers that were sent unsolicited commercial text messages on their cell phones. See *Shen v. Distributive Networks LLC*, N.D. Ill., No. 1:06-cv-04403, settlement preliminary approval, 1/31/2007. The ruling results from unsolicited text messages that were allegedly sent from a variety of websites controlled by Distributive Networks LLC, a wireless content and technology company. Under the class action settlement plan, the company, which denies all allegations, would pay up to \$150,000 in compensation and attorneys' fees to settle the suit as well as be required to comply with consumer marketing guidelines.

An article about this case is available at:

<http://pubs.bna.com/ip/BNA/EIP.NSF/7c407ecc8216ce4185256d05005e8b30/8f5afc01d0bb1a158525727a00826719?OpenDocument>; the full text of the opinion is available at: <http://pub.bna.com/eclr/06c4403.pdf>.

- **Congressional Committee Questions FTC About Rise in Spam** – The newly convened House Energy and Commerce Committee has focused their attention on CAN-SPAM. Members of the Committee sent a letter to the FTC asking for the Commission's comments as to whether any legislative changes are needed to address the rise in spam. The letter references a recent Postini report that found that spam has increased more than 100 percent since December of 2005, and suggests that the federal CAN-SPAM Act of 2003 may need amendment. The letter was signed by Subcommittee Chairman Bobby Rush (D-IL), ranking member Cliff Stearns (R-FL), and subcommittee members Gene Green (D-Texas) and Heather Wilson (R-NM). Lois Greisman, Associate Director of the FTC's Division of Marketing Practices, responded that the FTC already has "very strong enforcement tools" that have allowed the FTC to bring almost 90 spam cases to date.



In their letter, Committee members suggested that hearings may be necessary to address the issue, although the Committee's initial press statement in early January did not identify spam as a priority. We will continue to monitor this issue and will report if any hearings are scheduled.

An article about this development is available at:
<http://pubs.bna.com/ip/BNA/EIP.NSF/c7762b49479f833085256b57005afd29/993540133d2693678525727a008266d1?OpenDocument>, and a copy of the letter is available at:
<http://pub.bna.com/eclr/ftcletter013007.pdf>.

Postini's initial press release on its survey is available at:
http://www.postini.com/news_events/pr/pr011007.php

- **PayPal Describes Anti-Phishing Techniques** – In a recent interview, PayPal's Chief Information Security Officer, Michael Barrett explained how the company, a frequent target of phishing scams, is working to address these assaults. Included among PayPal's strategies are user education and the launch of authentication procedures that provide consumers with security keys for secondary authentication.

These strategies are useful tools for other companies that may also be targets of phishing scams but have not developed a company response to potential attacks. A strategy to address such scams is important for companies as consumers are increasingly falling victim to such attacks. One study reported that as many as 59 million phishing email messages are sent each day, with as many as 10 million being opened by consumers. False social networking site emails had the highest open rates, although financial institutions and payment services had the highest number of fraudulent emails associated with their sites.

An article with excerpts of the PayPal interview is available at:
<http://www.pcworld.com/article/id,128953-c.cybercrime/article.html>.

An article discussing the open rates for phishing emails is available at:
<http://www.clickz.com/showPage.html?page=3624876>.

V. TELECOM/WIRELESS

- **Anti-Pretexting Legislation in Congress Now Focusing on Carriers** – On February 7, 2007, Representatives Inslee (D-WA) and Blackburn (R-TN) introduced H.R. 852, the Consumer Telephone Records Protection Act of 2007. If enacted, the measure would make it illegal to obtain consumer phone records under false pretenses, give the FTC authority to prosecute violators, and require carriers to notify their customers of any unauthorized phone records disclosures. On February 8, 2007, Representative Dingell (D-MI) introduced his own similar measure, H.R. 936, the Prevention of Fraudulent Access to Phone Records Act, which, like H.R. 852, would also make it illegal to obtain consumer phone records under false pretenses and authorize the FTC to prosecute



violators. Additionally, Representative Dingell's measure would require that subscribers "opt in" to the sharing of their phone data before a carrier could share that information with a joint venture partner, contractor, or a similar third party. These measures – and others like them in the Senate – are notable in that they go beyond the anti-pretexting legislation enacted by Congress last year by imposing requirements on carriers, not simply on wrongdoers.

Additional information about H.R. 852 and H.R. 936 can be found at:
<http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.852>; and <http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.936>.

- **FTC Sues Pretexters to Enforce Provisions of Communications Act** – On February 15, 2007, the FTC filed a complaint in U.S. District Court to halt the operations of an entity alleged to have routinely engaged in the practice of pretexting. Most notable about the FTC's complaint is that it sought to enforce certain consumer protection provisions of the Communications Act – ordinarily the province of the FCC – pursuant to the FTC's broad authority to combat unfair or deceptive acts or practices under Section 5 of the FTC Act. The complaint is consistent with the recent trend of FTC enforcement actions relating to Section 5 where FCC enforcement efforts in the past have been more lax.

Additional information about the FTC's action is available at:
<http://www.ftc.gov/opa/2007/02/arg.htm>.

- **"Anti-Spoofing" Measure Approved by House Judiciary Committee** – On February 7, 2007, the House Judiciary Committee approved H.R. 740, the Preventing Harassment through Outbound Number Enforcement (PHONE) Act of 2007, which would prohibit the transmission of false Caller ID information with the intent to deceive the call recipient, a practice commonly referred to as "spoofing." The measure, introduced by Congressman Scott (D-VA), would punish violators with fines or potential prison terms of up to five years, as well as through forfeitures. Law enforcement agencies would be exempt from the Act, but it would apply to all types of phone service, including VoIP service. No date has been scheduled yet for full House consideration of the measure.

Additional information about H.R. 740, including the text of the legislation is available at: <http://thomas.loc.gov/cgi-bin/thomas>.

VI. CONSUMER PROTECTION

- **Bill Would Increase Child Pornography Penalties for ISPs** – Senators John McCain (R-AZ) and Chuck Schumer (D-NY) and Representatives Steve Chabot (R-OH) and Nick Lampson (D-TX) introduced a bill that would improve the system used by Internet service providers to report the transmission of child pornography over their systems and make the failure to report the pornography a federal crime subject to higher fines (\$150,000 for the first failure to report and \$300,000 for the second and subsequent failures). The proposed Securing Adolescents from Exploitation-Online (SAFE) Act of



2007 would also expand the range of companies obligated to make the reports, which are sent to the National Center for Missing & Exploited Children. The bill would apply to any provider of an electronic communication service, defined in the bill as any service which provides to its users the ability to send or receive wire or electronic communications.

The Senate bill is available at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:s519is.txt.pdf; the House bill is available at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h876ih.txt.pdf.

VII. STATE LEGISLATIVE AND ENFORCEMENT ACTIVITIES

- Washington Files Another Spyware Complaint – On February 7, the Washington Attorney General filed another spyware case, the fifth such lawsuit filed by the state using their Computer Spyware Act of 2005 and its consumer protection laws. These California-based defendants, SecureLink Networks and its chief executive officer, Manual Corona; NJC Softwares and officer Rudy O. Corella; and FixWinReg and its president, HoanVinh V. Nguyenphuoc, are accused of sending false and misleading messages, including the misrepresentation of operating system messages, modifying computer settings, and inability to uninstall the software.

The Attorney General's press release and link to the complaint are available at: <http://www.atg.wa.gov/pressrelease.aspx?&id=12328>.

- **REAL ID controversy continues to brew** – As noted in the most recent *Privacy and Data Security Briefing*, several states are starting to oppose the obligations placed on them as part of the 2005 REAL ID Act. The REAL ID Act requires states to implement certain features in their driver's license/identity system to meet certain machine readable standards by 2008. The state criticisms are associated either with the unfunded mandate of the Act, privacy concerns with the creation of a de facto national identification card, the creation of a database and network to share the license information, or with the fact that the Department of Homeland Security has not yet released its regulations with which the states must comply.

U.S. Senator Susan Collins (R-ME) said on February 9 that she will introduce federal legislation to delay the implementation of the federal law. The ACLU also announced its opposition to the REAL ID Act, and have been testifying in front of state legislatures on this issue.

An illustrative sample of the state resolutions, bills, and memorials calling for the repeal of the REAL ID Act or refuse to implement it are available at: Arizona--S.M. 1003 <http://www.azleg.gov/legtext/48leg/1r/bills/sm1003p.pdf>; Georgia--Sub. S.B. 5 http://www.legis.ga.gov/legis/2007_08/pdf/sb5.pdf; Hawaii--S.C.R. 29 http://www.capitol.hawaii.gov/sessioncurrent/Bills/SCR29_.pdf; Maine--S.P. 113, as



agreed to, is available at <http://op.bna.com/pl.nsf/r?Open=dapn-6xsqjd>; Maryland--S.J.R. 5 <http://mlis.state.md.us/2007RS/bills/sj/sj0005f.pdf>; Missouri--H.C.R. 20 <http://www.house.mo.gov/bills071/biltxt/intro/HCR0020I.htm>; Montana--H.B. 287 <http://data.opi.mt.gov/bills/2007/billpdf/HB0287.pdf>; New Mexico--H.J.M. 13 <http://legis.state.nm.us/Sessions/07%20Regular/memorials/house/HJM013.pdf>; Utah--H.R. 2 <http://le.utah.gov/~2007/bills/hbillint/hr0002.pdf>; Vermont--J.R.H. 2 <http://www.leg.state.vt.us/docs/legdoc.cfm?URL=/docs/2008/resolutm/JRH002.HTM>; Washington--S.J.M. 8005 <http://www.leg.wa.gov/pub/billinfo/2007-08/Pdf/Bills/Senate%20Joint%20Memorials/8005-REAL%20ID%20act.pdf>; Wyoming--H.J. 0008 <http://legisweb.state.wy.us/2007/Introduced/HJ0008.pdf>.

The ACLU statement is available at: <http://www.realnightmare.org/resources/106> (ACLU-supported website).

VIII. INTERNATIONAL ACTIVITIES

UK Regulator Fines Bank \$1.9 Million over Laptop Theft and Inadequate Security in First Data Breach

In the first penalty assessed in the UK for lax security, the UK Financial Services Authority ("FSA") fined The Nationwide Building Society ("Nationwide") -- a mortgage lending and banking services institution -- \$1.9 million for what it determined to be inadequate security measures, failing to respond to the theft of an employee's laptop that contained personal information relating to 11 million of Nationwide's customers, and potentially exposing customers to an increased risk of financial crime. The FSA stated in its Final Notice that the fine was issued because Nationwide breached Principle 3 of the FSA's Principles for Business which provides that "[a] firm must take reasonable care to organize and control its affairs responsibly and effectively, with adequate risk management systems." The FSA determined that Nationwide's violation of this Principle was due to the bank's failure to adequately assess the risks in relation to the security of customer information, information security procedures which failed to adequately and effectively manage the bank's risks, the bank failed to implement adequate training and monitoring to ensure its information security procedures were disseminated and understood by employees, and the bank failed to implement adequate controls to mitigate security risks. An FSA spokesperson noted that the fine was not being imposed due the "fact of the theft itself, but because of the wider control failings we discovered with the bank as a result of the investigation afterwards" and that the FSA's further intent was to send a message to the banking industry that it takes security issues very seriously.

A critical lesson to take away from this action is that rather than the Information Commissioner, the UK's data protection authority, taking action against Nationwide, the FSA stepped in and essentially overrode application of the Data Protection Act 1998, which grants limited power to the Information Commissioner and limits penalties to approximately \$9,700 per violation. The fact that other regulators are willing and able to step in and assess much larger penalties should provide further incentive for business to



audit their data protection and security functions, including employee training, policies and system security, and take any necessary corrective actions.

For the full text of the FSA's Final Notice see: <http://www.fsa.gov.uk/pubs/final/nbs.pdf>.

IX. RADIO FREQUENCY IDENTIFICATION TECHNOLOGIES (RFID)

- **RSA Conference 2007 Addresses "Legislate or Innovate" Debate Affecting RFID Technologies** – Members of the RSA Conference 2007 panel, "RFID – The benefits and the challenges: Do we legislate or do we innovate?" warned against self-defeating privacy and security legislation for RFID technologies. Ari Juels, Principal Research Scientist at RSA Laboratories said, "[t]echnologically prescriptive legislation is inappropriate and likely to be ineffective and likely to hamper technology with enormous promise. Scientists at this point don't know the right solutions to privacy and security problems in RFID infrastructure and its equally or more difficult for legislators to anticipate them, so legislation that includes specific prescriptive technological provisions is likely to be self-defeating."

Notably, the U.S. government has a long history of using RFID technologies, but Robert Cresanti, Under Secretary at the Department of Commerce, offered that the government has not generally been in the business of setting standards. Instead, Cresanti noted that the government has generally relied on industry working groups to establish standards, and he suggested that allowing such groups to evolve privacy and security standards might be the appropriate mechanism from a consumer perspective. Similarly, Toby Stevens, Director of the UK-based Enterprise Privacy Group, indicated that effective industry self-regulation might be the best option for avoiding "counterproductive legislation."

While the experts in this area caution against premature legislation, legislative efforts are a response to privacy groups' concerns regarding the proliferation of RFID technologies to achieve unauthorized access to private and confidential information. What seems clear in this debate is that the security and privacy issues raised by RFID technologies will continue to receive attention as the various stakeholders vie for some level of control over the outcome.

An article on this issue is available at:
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1242602,00.html



February 22, 2006 – March 7, 2006.

I. PRIVACY

- **Government Has Easy Access To Stored Data** – The Center for Democracy and Technology (CDT) released a report on February 22, calling for legislation to update the 1986 Electronic Communications Privacy Act, specifically to protect consumers' personal information held by Internet service providers (ISPs). The report acknowledged that ISPs have developed privacy policies to protect consumer information, but those policies usually have exceptions for government subpoenas. The report seeks legislation that would prevent the government from obtaining e-mail content or other stored communications without a search warrant. Currently, the government needs only a subpoena, which is issued without judicial approval, rather than a search warrant, which requires judicial approval based on probable cause that a crime has been or is being committed.

The CDT report is available at: <http://www.cdt.org/publications/digital-search-and-seizure.pdf>.

- **Amicus Briefs Filed In Google Case** – The CDT and two Stanford University law professors filed amicus briefs on February 24 in the ongoing legal battle over whether Google will have to disclose its customers' search results to the U.S. Department of Justice. CDT's brief argued that the Electronic Communications Privacy Act prohibits Google from disclosing such search results to the government, because Google's search engine qualifies as a "remote computing service" under the law, thereby requiring the government to seek a court order or search warrant before Google could turn over the information. CDT's argument is that customers who send their search inquiries to Google are no different than companies that outsource their payroll operations to a data-processing company, and should therefore receive the law's protection.

The professors' brief stated that the law is very complicated and unclear and argued that the court should allow privacy experts to explain the law to the court before ruling regarding Google's obligation to produce the data.

Google's brief, the Department of Justice's brief, and the amicus briefs are available at: <http://www.cdt.org/headlines/865>.

- **Government Interest In Data Mining Techniques Continues** – National Security Agency officials met with Silicon Valley venture capitalists in February to discuss new data mining tools, reviving privacy concerns about the use of such technology. In the wake of the discovery of President Bush's domestic surveillance program, the use of such technology is attracting renewed interest and concern about the government's information collection methods.



A February 25 article on this issue is available at:
http://news.com.com/Taking+spying+to+higher+level%2C+agencies+seek+ways+to+mine+data/2100-1028_3-6043296.html.

- **Minnesota Republican Party CD Collects User Data** – The Minnesota Republican Party plans to distribute a CD that advocates a ban on gay marriage and gathers data on those who view the CD. Test copies provided to the media contained no disclosures that data was being collected; however, party officials have stated that the final version of the CD, which will be mailed soon to hundreds of thousands of Minnesotans, will provide a notice that the information gathered will be shared with the party. Privacy advocates have also voiced concern that the collected data could be accessed by third parties, because the data collected by the test CDs was sent to an unsecured computer server. Again, party officials have indicated that the server will be secured when the final CDs are mailed. As data collection becomes more high-tech and moves from paper surveys to the automated data collection techniques like that used by the Minnesota Republican Party's CD, companies need to keep consumers informed about their data collection and security practices.

A March 2 article on this issue is available at:
<http://www.nytimes.com/aponline/technology/AP-Tech-Voter-Mining.html>.

II. SECURITY

- **CardSystems Settles FTC Investigation** – CardSystems Solutions, Inc., the credit card processor whose computer systems were hacked resulting in the exposure of 40 million credit card numbers and several million dollars of fraudulent purchases, signed a consent decree with the Federal Trade Commission on February 23, 2006. In its complaint, the FTC alleged that CardSystems' lack of security was an "unfair" trade practice. By relying on its authority to seek redress for unfair practices, the FTC needed to show that there was or was likely to be "substantial injury to consumers" that was not offset by countervailing benefits and was not reasonably avoidable by consumers. Though the FTC has said it will only use this authority to address data breaches when security failures are egregious, we are concerned that any data breach could result in "unavoidable" "substantial injury" to consumers and create potential liability under this theory.

Until recently, the FTC tended to rely more on its authority to investigate deceptive acts – typically commitments in a privacy policy that were not met. This is the third time the FTC has used this theory following a data breach. The first two enforcement actions were against BJ's Wholesale Club and DSW, Inc., both of which involved significant failures in data security.

The FTC's complaint enumerated the security failures of CardSystems, including:

1. Storing information "in a vulnerable format" for up to 30 days;



2. Failing to assess the vulnerability of web application and computer network to common attacks;
3. Failing to implement "simple, low-cost, and readily available" defenses to such attacks;
4. Failing to use strong password protection;
5. Failing to use readily available security measures to limit access between computers on its network and between such computers and the Internet; and
6. Failing to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations.

While this list should not be viewed as an exhaustive overview of the missteps that can lead to an FTC investigation, it does illustrate the kinds of failures that, when taken together, may lead to liability in the event of a breach. Without a breach or some other consumer harm, the FTC is not able to bring a complaint under this theory.

The consent decree requires the company to implement a comprehensive information security program and obtain an independent audit of its security program every two years for the next 20 years. CardSystems is no longer in business and recently sold its assets to a California company Pay By Touch, which must also abide by the terms of the consent decree.

The complaint and consent are available at:
<http://www.ftc.gov/os/caselist/0523148/0523148.htm>.

III. SPYWARE

- **Symantec Settles Suit With Adware Purveyor Hotbar.com** – On February 24, 2006, anti-spyware vendor Symantec dropped its lawsuit against Hotbar.com, Inc., which sought to affirm Symantec's position that Hotbar's programs were adware that could lawfully be considered security risks. Under the terms of the out of court settlement, Hotbar's programs will continue to be classified as adware, but Symantec will no longer recommend that users delete the programs. Instead, Symantec will classify Hotbar's adware as "low-risk" and recommend that users ignore the software. Symantec insists that the settlement is the result of its current understanding that users want guidance on making their own choice rather than a recommendation one way or the other. Critics, however, are criticizing the anti-spyware company for backing down to threats by Hotbar.

The complete *TechWeb News* article is available at:
http://www.cmpnetasia.com/oct3_nw_viewart.cfm?Artid=28396&Catid=5&subcat=50&action=News.

IV. SPAM



- Consumers Receiving Less Spam and Better Targeted E-mail** – A recent Epsilon Interactive survey of 1005 respondents reveals that 56% of responding consumers are now receiving less spam than they received last year. The majority of consumers (60%) report that the email communications they receive are more targeted and relevant than the communications they received from those same companies last year. These findings are coupled with the study's report that 75% of e-mail senders are using an anti-spam filter to ensure their e-mail's successful delivery. Notably, the survey states that the number of false positives resulting from ISP spam filters remained steady with 31% of consumers reporting that e-mail to which they have opted-in to receive is regularly ending up in their junk mail folders. This led 55% of users to check their junk mail folders for legitimate marketing messages. Notably, the study found that the number of marketers that encourage consumers to add their company to consumers' address books (approximately 42%) remained unchanged between 2005 and 2006 meaning that more than half of all marketers are missing out on enhanced white-listing opportunities.

A press release announcing the findings is available at: http://www.epsiloninteractive.com/eisite/pressroom/press_releases/pr2006/pr-02-21-06.htm. A copy of the report can also be obtained on the same Epsilon Interactive website.

- Groups Come Together to Protest AOL's Goodmail Plan** – Electronic Frontier Foundation (EFF) and MoveOn.org have brought together numerous nonprofits and other business to fight America Online's new guaranteed e-mail delivery program. See February 7 and 21, 2006 *Privacy and Data Security Briefings* for details regarding the new program. As part of this effort they have launched a website, www.dearaol.com, which provides an online petition users can sign asking AOL to change its policy. As previously reported, Yahoo also plans to implement a fee-based guaranteed e-mail delivery system. However, the group has focused on AOL because its program is further along and broader in scope than Yahoo's program. AOL expects to implement the new system within a month whereas Yahoo will test its service a few months later and charge fees only to e-mails that relate to purchases or financial transactions.

Opponents maintain that the fee-based system puts non-participants at a competitive disadvantage without providing any improvements for consumers in stopping spam. They complain that AOL will reduce the quality of service on the free system and focus their spam filtering efforts on the new program. This would mean that consumers can expect to encounter more false positives for legitimate e-mail from non-participating companies. This has raised the ire of nonprofits and others who maintain they will not be able to pay the fees.

Other activists have come out against the attack on AOL characterizing the opposition groups as spammers themselves and maintaining that the opposition effort is unreasonable and unbalanced.



Late last week, AOL also responded by stating that it would pay the fees of non-profits that employ a third party to prove that the non-profit does not spam. While it is not clear what company AOL will work with to provide the non-profit service, companies like Bonded Sender employ such a service by charging non-profits a \$400 application fee and \$250 yearly bond to ensure they are not spending spam. These non-profits are limited to one million messages a month with fees increasing as the number of e-mails increase.

We will continue to monitor this issue as it unfolds. An article highlighting the latest developments is available at: <http://www.nytimes.com/2006/02/28/technology/28mail.html?ei=5089&en=87fbd0edd5183d71&ex=1298282800&partner=rssyahoo&emc>.

- Chinese Government Acts to Stop Spam** – In recognition of findings that show China as second only to the United States in the number of spam e-mails sent, China's Ministry of Information Industry (MII) adopted new e-mail service regulations to combat the sending of spam. The regulations will take effect on March 30, 2006 and allow only those with Internet value-added services (VAS) licenses to provide e-mail services in the country. The regulations also state that companies sending unsolicited e-mails without an "Ad" or "Advertising" heading will lose their licenses while senders without a license could receive penalties of up to \$3,750. Additionally, MII launched a reporting center where Internet users can register complaints against spammers.

MII is applying similar regulations to Short Message Service (SMS) spam under which mobile users will be required to register with their real names in order to send text messages through their cell phones.

It is not clear that the MII's actions will impact the international rate of spam, given the loose guidelines, the various national laws governing commercial email, and the MII's comparative lack of enforcement capacity.

An article highlighting this development is available at: <http://www.digitalmediaasia.com/default.asp?ArticleID=13602>.

V. STATE ACTIVITIES

State legislative activity has increased, both in terms of introduced as well as passed legislation, which should continue until about mid-year, when many state legislatures adjourn. We will try to keep you up-to-date on the major developments in state-related issues.

- Do-Not-Mail Bills Introduced in Three States** – Following on the heels of the success of the federal Do-Not-Call registry, and the Children's Protection Registry Acts discussed in previous *Briefings*, Illinois, Michigan, and New York have introduced "do-not-mail" bills attempting to regulate commercial mail. The Direct Marketing Association (DMA) has joined a coalition spearheaded by the Association for Postal Commerce to lobby against these bills. The bills are not likely to pass any of the legislatures at this time.



The DMA article is available at: http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=35835

- **Arizona Close to Data Breach Notification Law** – The Arizona Senate followed the lead of several of its neighbors in passing a data breach notification bill. The bill has been sent to the House for consideration. Passage is expected shortly, given that the state has the highest per-capita rate of identify theft complaints, according to the FTC. Many of those thefts involve preying upon older residents through traditional means of theft, but the fear of online theft has heightened Arizonan attention on this issue.

The bill as passed the Senate is available at:
<http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/legtext/47leg/2r/bills/sb1338s.htm>.

VI. INTERNATIONAL AFFAIRS

- **EU Approves Controversial Data Retention Directive** – The Data Retention Directive, enacted as a means to fight terrorism and organized crime, was passed by justice ministers in Brussels on February 21. Telecommunications and internet service providers are now be required to maintain details of customers' communications for up to two years. The legislation applies to "traffic data" – information including data that can trace fixed or mobile telephone calls, time and duration of calls, location of the mobile phone being called, details of connections made to the internet, and details of email and internet telephony services – but not to the content of such communications. Traffic data must be stored and made available to law enforcement authorities for between six and 24 months, with service providers bearing the costs of storage under the Directive. Each EU Member State must adopt the Directive through its own national legislation by August 2007. Though this legislation has been formally approved, it is anticipated that there will be legal challenges. Ireland has threatened to challenge the Directive before the European Court of Justice on the basis that the legislation does not fall under the legal competence of the EU, and is strictly a national government decision. In addition, the EU Data Protection Supervisor has criticized the directive for not sufficiently addressing the access to data by individuals nor the data's further use once it has been accessed by law enforcement authorities.

For additional information see the 2/21/06 press release from Justice and Home Affairs, page 8, available at: http://ue.eu.int/ueDocs/cms_Data/docs/pressData/en/jha/88467.pdf.
http://news.com.com/EU+data+retention+directive+gets+final+nod/2100-7348_3-6042032.html.



- **UK Issues Guidance to Professionals on Maintaining Opinions** – The UK Information Commissioner's Office recently issued guidance to professionals regarding access to opinions contained in their files. Professionals that record their opinions in peoples' files in the course of their work, such as educators and doctors, now have new guidance about complying with the Data Protection Act, the UK's implementation of the EU Data Protection Directive. The ICO stated that the Act gives everyone the right to review information held about them, including opinions. The ICO's recent guidance instructs professionals to make it clear that the information is an opinion as well as who gave it and when. In addition, opinions should be accurate, up to date and contain enough information to be correctly interpreted. Finally, a policy should be in place detailing how long and for what reasons the opinions should be retained. If these guidelines are followed, opinions cannot be challenged for inaccuracy under the Act simply because it is different to an opinion held by someone else, though factual information contained within an opinion can be challenged.

The ICO Data Protection Good Practice Note is located at
http://www.ico.gov.uk/cms/DocumentUploads/Opinions_GNP_28_Feb_06_V2.pdf.

VII. TELECOM/WIRELESS

- **House and Senate Judiciary Committees Approve Legislation Banning Pretexting** – On March 2, 2006, the House and Senate Judiciary Committees separately approved bills criminalizing the practice of pretexting (*i.e.*, using fraudulent means to acquire consumer telephone records and related information). The bills – S. 2178 and H.R. 4709 – would impose penalties on violators consisting of prison sentences, fines, or both. Similar bills have been discussed and in some cases introduced in Congress, but the bills approved by the House and Senate Judiciary Committees appear for now to be the frontrunners. It is not clear when they may be acted on by the full Senate and House. The FCC separately is investigating the practice of pretexting, but is generally looking to Congress to develop additional restrictions and penalties not currently authorized under Section 222 of the Communications Act, the provision governing Customer Proprietary Network Information, or "CPNI."

Copies of S. 2178 and H.R. 4709 are available at:
<http://thomas.loc.gov/cgi-bin/query/D?c109:2:./temp/~c109phKNBS> and
<http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.4709>, respectively.

- **FTC Fines Book Club Marketer \$680,000 for Do-Not-Call Violations** – On February 23, 2006, the FTC entered into a consent decree with Bookspan, a book club direct marketer, fining the company \$680,000 for its failure to comply with the national do-not-call list and Bookspan's own company-specific do-not-call list.

The FTC's press release and additional information about this case, including the consent decree, are available at:



<http://www.ftc.gov/opa/2006/02/books.htm>.

VIII. DO-NOT-FAX

- **California Court Strikes Down Signed Writing Requirement for Interstate Commercial Faxes** – On February 27, 2006, a Federal District Court in California issued a declaratory ruling striking down a portion of a SB 833, the California law (that was scheduled to go into effect on January 1 but had been stayed) requiring entities to secure express written consent prior to transmitting commercial faxes to or from locations in California. The ruling pertained only to interstate fax transmissions, and the extent to which intrastate fax transmissions are affected is not yet clear.

This appears to be the first time a noteworthy judicial body has addressed the extent to which federal telemarketing and fax laws preempt more restrictive state laws intended to govern interstate transmissions. Although other aspects of this case remain pending and the court's decision may be appealed, this appears to be a positive development for businesses and organizations that would like to see a single regulatory regime governing interstate telemarketing and fax transmissions. The issue also is before the FCC in connection with a pending Petition for Declaratory Ruling filed by the Fax Ban Coalition in 2005.

The declaratory ruling in no way negates existing federal telemarketing and fax obligations, including do-not-call obligations and the requirement that an entity have an established business relationship with (or consent from) a recipient in order to transmit a commercial fax to that recipient. The court's decision is attached to this *Briefing* as a pdf document.

- **FCC Proposes \$776,500 Fine to Health Network Provider for Fax Violations** – On February 28, 2006, the FCC issued a Notice of Apparent Liability and Forfeiture against First Choice Healthcare, Inc., in the amount of \$776,500 for willful and repeated fax violations. First Choice apparently transmitted at least 98 unsolicited advertisements via facsimile to at least 37 individuals without proper authorization, and after receiving a citation (warning) from the FCC in connection with these activities. The FCC's action against First Choice is consistent with the strict approach it has taken in recent years in connection with fax violations.

A copy of the FCC's Notice of Apparent Liability and Forfeiture is available at: <http://www.fcc.gov/eb/Orders/2006/FCC-06-22A1.html>.



March 6, 2007 – March 19, 2007.

I. PRIVACY

- **Google Revises Data Retention Policy** – Google announced a revised data retention policy on March 14 in a posting on its official blog. Google keeps logs of all searches with digital identifiers linking the searches to specific computers and Internet browsers; Google currently keeps such logs indefinitely. Under the new policy, Google will purportedly “anonymize” such logs after 18 to 24 months by stripping out the last four digits of the IP addresses collected. The abridged IP addresses will likely be associated with on-going searches, therefore it is unclear how this would provide additional privacy protections to Google users.

Google stated that it was making this change after receiving feedback from privacy advocates, regulators, and users. Google appears to have made the change in part based on its conversations with Norwegian Data Protection Authority, which has been investigating Google for purported Data Protection violations. The change will not be implemented for approximately a year.

While the changes were intended to allay privacy concerns, privacy advocates have had mixed reactions. Ari Schwartz of the Center for Democracy and Technology, praised Google for attempting to compromise between collecting data and protecting users' privacy. However, Marc Rotenberg of the Electronic Privacy Information Center, stated that the 18 to 24 month time frame is too long and that because of Google's dominant position, this will become the expected standard for data retention.

The announcement on Google's official blog is available at: <http://googleblog.blogspot.com/2007/03/taking-steps-to-further-improve-our.html>.

Articles on this issue are available at: http://www.nytimes.com/aponline/technology/AP-Google-Privacy.html?_r=3&oref=slogin&oref=slogin and <http://www.informationweek.com/news/showArticle.jhtml?articleID=198001087>

II. SECURITY

- **Federal Trade Commission Issues Business Guidance on Data Security** – The Federal Trade Commission issued a new set of guidelines on safeguarding personal information for businesses. The guide suggest businesses:
 - Take stock of the information they are collecting and storing;
 - Only retain the information they needed for business or legal purposes;
 - Protect the information they store;
 - Properly dispose of information that is no longer needed; and
 - Develop a plan to respond to data security breaches.

The guide includes more specific recommendations in each of these categories. The bulk of the guide, however, is devoted to steps companies can take to protect information they



retain, reflecting the FTC's focus on requiring businesses to take reasonable steps to protect sensitive information. Substantial failures to take these steps could result in liability under Section 5 of the Federal Trade Commission Act. In announcing the release of the guide, Chairman Deborah Majoras noted that of the fourteen enforcement actions the FTC has brought against companies that the FTC believed failed to adequately protect consumer data, "none was a close call."

The guide itself, of course, contains only voluntary recommendations and does not constitute new rules issued by the FTC.

A copy of the guide is available at: <http://www.ftc.gov/infosecurity/>

- **Senator Pryor Introduces Federal Credit Freeze Legislation** – On March 7, 2007, Senator Mark Pryor (D-AR) introduced S.806, the Consumer ID Protection and Security Act. The Act would create a national framework for consumers to place "credit freezes" on their accounts if they believe their personal information may have been compromised. The bill would primarily affect credit reporting agencies which would have additional reporting and recording keeping requirements. Businesses that seek to open credit lines for consumers, however, may see an increase in administrative costs under the bill.

Many states now have credit freeze laws on the books and the debate over data breach notification legislation last year included disagreements over whether such legislation should include a credit freeze provision. Though it is still too early to tell, the existence of a separate credit freeze bill could remove one hurdle to passage of a data breach notification measure this year.

A copy of the bill is available at: http://thomas.loc.gov/cgi-bin/t2GPO/http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:s806is.txt.pdf

III. SPYWARE

- **FTC to Target Spyware Advertisers** – Federal Trade Commissioner Jon Leibowitz warns that the Commission plans to escalate its attack on spyware by going after the advertisers whose ads are served by spyware programs. Leibowitz said that the Commission will send letters to up to 200 major corporations that place the majority of such ads serving notice that they need to police where their ad dollars are going. The move follows on the heels of New York State's settlements with three large advertisers in January in which Cingular Wireless, Travelocity.com, and Priceline.com agreed to pay a total of \$100,000 in fines.

An article discussing this matter is available at: http://www.washingtonpost.com/wp-dyn/content/article/2007/03/05/AR2007030501475_pf.html.



- **Two Anti-Spyware Bills Introduced in the House** – Two "new" bills aimed at cracking down on spyware and other pernicious software were recently introduced in the U.S. House of Representatives

- H.R. 964, "Securely Protect Yourself Against Cyber Trespass Act" or the "SPY Act," would require companies to provide adequate notice and obtain consent from users before downloading their software onto consumers' computers. The legislation would also require that such software be easily removable and give the FTC the ability to impose greater penalties on violators. A version of the legislation has passed the House in the previous two Congresses but died both times in the Senate. Some commentators worry that the bill's definition of software may be too broad by bringing within its ambit cookies and other technologies that enable the efficient and seamless use of the Internet. Others believe the Good Samaritan provision, which aims to protect software providers that with consent attempt to disable or remove spyware, may provide a loophole through which bad actors can slip. The legislation has been referred to the House Committee on Energy and Commerce.
- H.R.1525, the "Internet Spyware (I-SPY) Prevention Act of 2007," has been reintroduced and referred to the House Committee on Energy and Commerce after failed attempts to pass a similar bill in the last Congress. The bill, sponsored by Reps. Zoe Lofgren (D-CA) and Bob Goodlatte (R-VA), aims to combat spyware and phishing schemes that attempt to trick consumers into revealing personal financial information. The legislation provides for fines and imprisonment up to five years for persons that intentionally access a users' computer without authorization or in excess of user authorization by downloading a computer program onto that computer for the purpose of defrauding the user or to further another criminal offense.

The text of H.R. 964 and other information regarding the legislation are available at: <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.00964:>

The text of H.R. 1525 and other information regarding the legislation are available at: <http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.1525:>

IV. SPAM

- **FTC Announces Plans to Hold Spam Workshop** – During a keynote address at the recent IAPP Summit, Chairman Deborah Majoras announced that the FTC will sponsor a public workshop to address spam sometime this summer. A similar conference was held three years ago.

Some industry leaders have suggested that this could mean that the FTC plans to propose additional legislative or regulatory solutions to address the increase in spam. As reported in the *February 21 Privacy and Data Security Briefing*, the House Energy and Commerce Committee has already sent a letter to the FTC asking for the Commission's comments as



to whether any legislative changes are needed to address the rise in spam. Calls for a new response to spam are likely to continue as security companies report that spam is on the rise. MessageLabs has just reported that “77.8 percent of all sent emails for the month of February from ‘new and unknown bad sources’ were spam.” This represents a reported 2 percent increase from January.

Notably the FTC has not issued final regulations under CAN-SPAM. When asked about the timing of the release of such regulations during a IAPP breakout session, an FTC staff person stated that they would be forthcoming, but did not offer a timeline. We will continue to monitor any new developments on a public workshop or the release of the final CAN-SPAM regulations.

A copy of Chairman Majoras’s speech is available at: <http://ftc.gov/speeches/majoras.htm>. A copy of a recent article noting rising spam is available at: http://www.consumeraffairs.com/news04/2007/03/spam_rates.html.

- **Microsoft Releases New Authentication Tool To Combat Phishing** – Microsoft has developed an Extended Validation Security Socket Layer (EV SSL) certificate program in an attempt to make it more difficult for phishers to create fraudulent websites. Under the new plan, third-party certification authorities, such as VeriSign and Entrust, are provided with guidelines for authenticating websites under which they may award the EV SSL certificate. Websites will buy the EV SSL seal from the third party certification authorities that will be tasked with ensuring that the relevant company has satisfied the guidelines, which include, for example, having a legitimate address and control of the Web domain in question.

Under the certificate program, EV SSL–certified sites will look a bit different from other secure sites, which currently display a “lock” icon in the Web browser. In contrast, when Internet Explorer reaches part of a website that meets the EV SSL standard, the address bar will turn green and the country where the website is based will be revealed.

Some companies, including PayPal, already have the certificate, and VeriSign reports that it has more than 300 businesses going through the certification process.

An article about this development is available at: http://www.cio.com/archive/030107/tl_phish.html?CID=29084.

- **The Securities and Exchange Commission (SEC) Halts Trading as a Result of Spam Campaigns** – As part of a campaign called “Operation Spamalot,” the SEC suspended trading of the securities of 35 companies that were the subject of recent email campaigns. The emails at issue promoted small-company stocks with subject headers such as “Ready to Explode,” “Ride the Bull,” and “Fast Money.” The SEC maintains that an estimated 100 million of these types of spam messages promoting the stocks are sent weekly and may include inadequate and inaccurate information about the companies they promote. The emails have triggered dramatic spikes in the relevant share price and trading volume



and have resulted in investors losing money. The trading suspensions were imposed for ten (10) business days and will terminate on March 21, 2007.

The SEC’s report is available at <http://www.sec.gov/investor/35tradingsuspensions.htm> and an article about this development its available at: http://www.cio.com/archive/030107/tl_phish.html?CID=29084.

V. TELECOM/WIRELESS

- **FCC Adopts CPNI Rule Revisions; More Related Legislation Introduced in Congress** – It has been reported that the FCC on March 13, 2007, adopted revisions to its existing Customer Proprietary Network Information, or “CPNI” rules, which are intended to safeguard specific forms of consumer call data. The text of the FCC’s rule revision has not yet been released but is expected shortly. In a related development, Senator Pryor (D-AR) on March 6, 2007, introduced S.780, known as the “Protecting Consumer Phone Records Act,” which would require written consent prior to acquiring, using or offering for sale a person’s CPNI, whether maintained by a traditional telecommunications carrier or a provider of Voice-over-Internet Protocol service. The measure also would require service providers to notify consumers if their CPNI is improperly disclosed. Penalties of up to \$90,000 per day would apply for certain violations. S.780 is among several measures circulating in Congress addressing the CPNI issue.

A copy of S.780 can be found at: <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:s:00780>.

- **FCC Declines to Rescind EBR Exemption for Fax Advertisements** – On March 15, 2007, the FCC released an order declining to commence a rulemaking to consider rescinding the Established Business Relationship, or “EBR” exemption for unsolicited advertisements transmitted by fax. The request for a rulemaking pre-dated the enactment of the Junk Fax Prevention Act, which codified the EBR exemption for commercial faxes and thus constrained the FCC’s ability to rescind the exemption, which previously existed pursuant only to an FCC rule.

A copy of the FCC’s order can be found at: http://hraunfoss.fcc.gov/edocs_public/quickSearch/getResult.

- **Legislation Introduced to Reauthorize Funding for National Do-Not-Call Registry** – On March 6, 2007, Senator Pryor (D-AR) introduced S.781, the “Do Not Call Reauthorization Act,” which would extend the FTC’s authorization to collect fees from telemarketers to access the national Do-Not-Call Registry. The current law authorized such fee collections from 2003 through 2007 only. Senator Pryor’s measure would extend that authorization indefinitely.

A copy of S.781 can be found at: <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:s:00781>.

- **Anti-Spoofing Measures Continue to Move Through the Congress** – On March 15, 2007, the House Commerce Committee approved H.R. 251, known as the “Truth in



Caller ID Act," which would amend the Communications Act to make it illegal for individuals to transmit misleading or inaccurate Caller ID information for deceptive or fraudulent purposes. A similar measure was passed by the House in the last Congress, but the Senate never acted on it. It remains unclear whether the Senate will act on the issue in this Congress; but, in a related development, Senator Nelson (D-FL) on February 28, 2007, introduced S.704, known as the "Truth in Caller ID Act of 2007," which could become the vehicle for Senate action.

Additional information about H.R. 251 and S.704 can be found at: <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.00251>; and <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:s.00704>.

- **Congress and States Continue to Target Political "Robo-Calls"** – Various measures continue to be introduced in Congress to regulate or prohibit the transmission of autodialed prerecorded telephone calls – or "robo-calls" – that have certain political purposes. For example, on March 7, 2007, Representative Lofgren (D-CA) introduced H.R. 1383, which would prohibit the transmission of calls that are knowingly used to deceive a person regarding the time, place and manner of an election; voter qualifications or eligibility; the political party affiliation of a candidate; or the sponsor, endorser or sender of a political "robo-call." Measures also have been introduced in roughly 20 states that would directly ban the transmission of political messages using autodialers and/or prerecorded voices. Some of the most recent of such measures include HB-4237 in Michigan and SB-125 in Tennessee.

A copy of H.R. 1383 can be found at: <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.01383>.

VI. GRAMM LEACH BILEY

- **Agencies Issue New Model Form For Gramm Leach Bliley Notices** – After years of research and consumer testing, the Federal Trade Commission and a variety of banking regulatory agencies released a proposed new model form for the privacy notices required by the Gramm Leach Bliley Act (GLB). The model forms will not be mandatory, but will provide a safe harbor for companies that need to comply with the notice and opt-out provisions under GLB.

The notice forms are a significant departure from the model clauses in the existing rule. The proposed model notice includes an initial page summarizing the company's information practices in a standardized dashboard format. Page two provides additional details on information sharing practices required by GLB and a series of definitions. Page three provides consumers with information on opt-outs and a way for consumers to exercise those rights. Companies that do not share any information that requires offering an opt-out will not have to include the third page of the notice. Significantly, the model form will also allow companies to meet their notice and opt-out requirements for sharing data with affiliates under the Fair Credit Reporting Act.



Under the proposed rule, to qualify for the safe harbor, the notice will need to be printed on three single-sided pieces of 8.5 x 11 paper and be printed in an easily readable type font. The introduction to the rule contains specific recommendations for typefaces and font size.

Once the proposed rule is published in the federal register, which should happen in the next two weeks, interested parties will have 60 days to comment on the model notice forms. The agencies are seeking comments on a number of issues, including whether companies believe they can accurately disclose their information practices using the new form and whether they are likely to adopt the new form.

The Agencies intend for the rule to go into effect as soon as it is published in final form, which will allow companies to immediately switch to the new format. The safe harbor for companies using the current model clauses will remain in effect for one year following the publication of the final rule, after which those companies can no longer be assured of compliance with GLB unless they switch to the new model form.

A copy of the proposed rule is available at: <http://www.ftc.gov/os/2007/03/P034815InteragencyProposalforModelPrivacyFormFRN.pdf>

A Hogan & Hartson *Privacy Update* on this topic is available at www.hhlaw.com/privacy/.

VII. CONSUMER PROTECTION

- **Kmart Settles with FTC Regarding Gift Card Practices** – The FTC announced on March 12 that Kmart agreed to settle charges that it had engaged in deceptive practices in the marketing and sale of its gift cards. This is the FTC's first action involving gift cards, although several states have previously been active in this area. According to the FTC's complaint, Kmart advertised its gift card as equivalent to cash but did not disclose that dormancy fees of \$2.10 per month would be assessed after two years of non-use. K-mart also allegedly represented that the gift card would never expire; however the FTC argued that through the continued application of the dormancy fee, the card could effectively expire after months of inactivity. The FTC alleged that the disclosures on the card itself were inadequate – they appeared in fine print and in legalese on the back of the card. Additionally, consumers who purchased gift cards online were allegedly not able to see any pre-sale disclosures at all.

As of May 1, 2006, Kmart stopped charging the dormancy fee on its gift cards. The settlement requires Kmart to implement a program to refund the dormancy fees to affected consumers and to publicize the refund program on its website. In the future, Kmart must clearly and prominently disclose any expiration date and potential fees in any advertising and on the front of all gift cards. Kmart must also make such disclosures at the point of sale and before the purchase.



Commissioners Pamela Jones Harbour and Jon Leibowitz issued a separate statement, concurring in part and dissenting in part, stating that they concur in the decision to bring an action against Kmart, but dissent in part from the proposed settlement because they believe the remedy should include disgorgement of ill-gotten profits.

The FTC's interest in this area as well as states' actions regarding gift cards indicate that retailers must be aware of the potential pitfalls in connection with gift cards.

The FTC's press release and related documents are available at:
<http://www.ftc.gov/opa/2007/03/kmart.htm>.

An article on this issue is available at: <http://www.dmnews.com/cms/dm-news/legal-privacy/40357.html>.

VIII. RADIO FREQUENCY IDENTIFICATION TECHNOLOGIES (RFID)

- **European Commission Issues Proposals for RFID Strategy** – On March 15, 2007, after a year of extensive Europe-wide public consultation, the European Commission proposed a European policy strategy for developing a clear and predictable legal framework for RFID. The framework is intended to address ethical implications, the need to protect privacy and security, governance of RFID identity databases, availability of radio spectrum, the establishment of harmonized international standards, and concerns over the health and environmental implications. Under the policy strategy, the Commission will:
 - Create in 2007 an RFID Stakeholder Group to provide advice and assistance to the Commission in developing a European policy position concerning RFID applications.
 - By mid-2007, propose amendments to the e-Privacy Directive to take account of RFID applications, as part of the EU Telecom Rules' review.
 - Publish, by the end of 2007, a recommendation on how to handle data security and privacy of smart radio tags to EU Member States and stakeholders.
 - In association with the Stakeholder Group, analyze the economic and social effects of smart radio tags and other technologies, particularly focusing on privacy, trust, and governance, leading to an assessment of policy options and need for further legislative steps, by the end of 2008.

With regard to RFID privacy and security, the Commission has taken the position that “[p]rivacy and security should be built into RFID information systems before their widespread deployment (‘security and privacy-by-design’), rather than having to deal with it afterwards.” Presumably to help reduce barriers to uptake while such design occurs, the Commission plans to “support the development of a set of application-specific guidelines (codes of conduct, good practices) by a core group of experts representing all



parties.” Another position that appears in the Commission's policy is the intent to strengthen international contacts with the United States and Asia with regard to international standards of interoperability and standardization.

The European Commission policy strategy provides an interesting contrast to the “legislate or innovate” debate currently occurring in the United States, and which we reported on in the *February 21 Privacy and Data Security Briefing*. As discussed in that briefing, there have been calls for industry self-regulation in the U.S., but there have also been calls for legislation to protect privacy as the use of RFID technologies proliferates. It will be interesting to see whether and how the European policy strategy, which appears to support industry self-regulation over legislation, will impact the U.S. debate.

Additional information and background materials regarding this RFID development in the EU can be found at:
http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=3247.

An article discussing the European Commission policy strategy can be found at:
<http://www.pcworld.com/article/id,129871-page,1-c,technology/article.html>.

March 19, 2007 – April 3, 2007.

I. PRIVACY

- **GAO Seeks Privacy Protections in DHS Data Mining Program** – The Department of Homeland Security (DHS) is moving forward with its data mining program called Analysis, Dissemination, Visualization, Insight and Semantic Enhancement (ADVISE), discussed in a previous issue of the *Privacy and Data Security Briefing*, without conducting a privacy impact assessment (PIA). The Government Accountability Office (GAO) stated in its report to the House Appropriations Committee that while DHS has added security controls to the program, it has not yet analyzed the potential for the program to misidentify people or incorrectly link them to terrorism. DHS has argued that such an assessment is not yet necessary, but the GAO believes it is necessary in order to build controls into the system before it is put to use.

The conflicting positions of DHS and the GAO will likely be the subject of further inquiry in Congress, where federal data mining efforts have raised concerns and calls for greater oversight. Recently introduced legislation in the Senate would require a PIA before launching new programs like ADVISE.

Articles on this issue are available at: <http://fcw.com/article98039-03-23-07-Web> and <http://www.newsday.com/news/local/longisland/politics/ny-ushome225139789mar22,0,5756989.story>.



- **Ponemon Institute Releases Results of Corporate Privacy Survey** – The Ponemon Institute, a privacy think tank, surveyed more than 7,000 web users, asking them to pick up to five companies they respect the most and the least for privacy practices, based on users' perceptions of how the companies collect, use, and protect personal information, including names, addresses, telephone numbers, and Social Security numbers. For the second year in a row, American Express is the top company, according to the survey results, followed by Charles Schwab and IBM. Other top companies include AOL, Amazon.com, eBay, and Google. Clearly defined policies and practices regarding data collection and use were key factors in the high scores achieved by those companies. On the other hand, data breaches and the overuse of online marketing tools such as pop-up ads hurt some companies' scores.

An article on this issue is available at:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9014698&intsrc=hm_list.

- **Massachusetts Secretary of State Claims Governor's Website Violates Privacy of Voters** – The Massachusetts governor's website requires visitors to register and provide their name and phone number, whereupon the website then provides a street address to ensure that it has identified the correct person. The Secretary of State, whose office oversees elections, was concerned that anyone could enter a name or phone number of someone else and then see that person's address. In response to the concern, the website now reveals only street names, and not house and apartment numbers. However, neither the ACLU nor the Secretary of State is convinced that this step has fully allayed the privacy concerns at issue.

Confirming people's identity by disclosing personal information and asking the individual to confirm it clearly raises privacy concerns and fails to meet basic standards for authentication, in the opinion of the Secretary of State. As the Secretary of State's inquiry shows, such activities are also likely to garner attention. Companies are strongly advised not to follow such authentication procedures.

An article on this issue is available at:

http://www.boston.com/news/local/massachusetts/articles/2007/03/27/galvin_sees_privacy_issue_on_patrick_site/.

II. SECURITY

- **Senate Judiciary Subcommittee Holds Hearings on Identity Theft** – The Senate Committee on the Judiciary's Subcommittee on Terrorism, Technology and Homeland Security held a hearing to discuss ways to address the growing problem of identity theft. The hearings were chaired by Senator Diane Feinstein (D-CA), who has introduced S.239, which would require companies to notify consumers of a breach involving their unencrypted personally identifiable information. Senator Feinstein used the hearing as a chance to promote immediate passage of S.239, even as a standalone measure. Senators



Patrick Leahy (D-VT) and Arlen Specter (R-PA) have introduced S.495, a more comprehensive data security bill that contains many of the same provisions in S.239. The House Judiciary Committee is currently reviewing S.495 to determine whether or not to introduce similar legislation on the House side.

Other highlights of the hearings included testimony by Federal Trade Commission Bureau of Consumer Protection director Lydia Parnes. Much of Parnes' testimony focused on the need to protect Social Security numbers. Limitations on the collection, use and disclosure of Social Security numbers have been a regular part of the data security debate on Capitol Hill. We continue to advise companies to review their use of Social Security numbers and, when feasible, eliminate the use and storage of this data. In addition to triggering virtually all state breach notification laws if the data is lost or stolen, Social Security numbers are subject to a variety of other state law restrictions and are likely to see increase federal oversight in the future.

Testimony from the hearing is available at:

<http://judiciary.senate.gov/hearing.cfm?id=2582>

- **Scope of TJX Breach Widens and Lawsuits Increase** – TJX, which operates T.J. Maxx and other stores in the United States and the United Kingdom released in recent SEC filings detailed information about a breach it suffered over the course of several years. The breach was caused by hackers placing software on TJX's systems that allowed them to download files containing at least 45.7 million debit and credit card numbers. The recent SEC filings also disclosed the following information.
 - The hackers had access to TJX's decryption tool, defeating any encryption measures the company put into place. While it is impossible to say what additional safeguards TJX had in place to protect the decryption algorithm, this disclosure highlights the need to separate decryption technology from the encrypted data and taken additional steps to safeguard the algorithm.
 - In the fourth quarter of 2007, the company spent \$5 million responding to the breach, which includes costs incurred to investigate and contain the breach, enhance computer security and systems, and communicate with customers, as well as technical, legal, and other fees.
 - The company currently faces class action law suits in state and federal courts in Alabama, California, Massachusetts and Puerto Rico, and in provincial Canadian courts in Alberta, British Columbia, Manitoba, Ontario, Quebec and Saskatchewan.
 - In addition, the company faces a lawsuit in federal court in Massachusetts on behalf of all financial institutions that issued credit and debit cards used at TJX stores during the period of the security breach. Many of these financial institutions will reissue hundreds of thousands of cards and are seeking restitution from TJX for those costs.
 - The Arkansas Carpenters Pension Fund, which holds shares of TJX, has commenced an action in the Delaware Chancery Court seeking access to TJX's



records regarding its response to the breach. This suit is a potential precursor to an investor class action law suit.

- o TJX also faces government investigations by the Federal Trade Commission, 30 state attorneys general, and several privacy commissioners in Canada.

While the TJX breach is the largest breach to date and involves intentional hacking, rather than the inadvertent loss of data, the range liabilities now faced by the company are illustrative. Federal and state regulators, as well as class action attorneys, closely examine any reported data breach and are prepared to investigate or file suit. The scope of potential harm caused by the TJX breach will also undoubtedly fuel calls for federal legislation to provide greater oversight on data protection in the private sector.

A copy of the SEC filing is available at: <http://ir.10kwizard.com/files.php?source=487>

III. SPAM

- **Utah Child Protection Registry Act Survives CAN-SPAM Preemption Challenge** – The U.S. District Court for the District of Utah has held that Utah's Child Protection Registry Act, which makes it a crime to send e-mail promoting sexually explicit materials to addresses registered as accessible to children, is not preempted by CAN-SPAM. *See Free Speech Coal. Inc. v. Shurtleff*, D. Utah, No. 2:05-cv-949, 3/23/07.

Under Utah Code §13-39-202, parents in Utah may register their child's electronic "contact points" with a state-administered registry service. Once registered, it is unlawful for anyone to email the contact point if the communication "has the primary purpose of advertising or promoting a product or service that a minor is prohibited from purchasing . . . or . . . contains or has the primary purpose of advertising or promoting material that is harmful to minors . . ." Utah Code §13-39-202(1). Under the law, marketers must pay a fee to scrub their lists against registered contact points before promoting content that is unlawful for minors in Utah to receive. Utah Code §13-39-201.

In considering the law, the court held that the Utah statute fell within the CAN-SPAM Act's preemption exception for state computer crime laws, 15 U.S.C. §7701(2)(B). The court stated that "CAN-SPAM's exception for computer crimes . . . is an express acknowledgment that criminal provisions regarding public welfare are within the province of the state's police powers." The court found that the registry law advances the state's interest in safeguarding parents' prerogatives in child rearing, and the statute explicitly defines violations of the law as "computer crimes." The court also rejected challenges to the statute under the dormant Commerce Clause and First Amendment challenges to the Utah law.

A copy of the court's opinion is available at: http://pub.bna.com/eclr/05cv949_032307.pdf



- **MySpace Files Phishing and Spam Suit Against Sanford Wallace** – On March 27, MySpace announced that it had filed a complaint in United States District Court for the Central District of California against Sanford Wallace, the notorious "King of Spam" for violations of state and federal laws including the CAN-SPAM Act and California's anti-spam and anti-phishing statutes. In its complaint, MySpace alleges that since October 2006 Wallace has perpetrated a phishing scam in an attempt to access MySpace user profiles. In his scam, Wallace created profiles, groups, and forums on the MySpace website in which he directed users to websites that Wallace owned or operated. In addition to carrying out the phishing scam, Wallace spammed thousands of users with advertisements that promoted his websites. The MySpace suit seeks a permanent injunction barring Wallace and his affiliated companies from the MySpace website as well as monetary damages.

Wallace is well-known for his use of the Internet for fraudulent schemes and has already been sued by America Online, Concentric Network Corp., CompuServe, and the FTC.

An article noting this development is available at: <http://www.latimes.com/technology/la-fi-briefs27.6mar27,1,3560821.story>

- **Phishing Scams Continue to Spread, Banking Customers Are the Most Frequent Targets** – Internet monitoring firm Cyveillance, Inc. released a study in which it found that number of sites targeted by phishing attacks grew 50 percent in the first two months of 2007, from 800 to 1,200. The study also found that Internet scams are combining phishing with malware by using phishing emails to draw users to websites that install malware on the email recipients' machines, in some instances without requiring any user action. According to Cyveillance, there may be thousands of malware-based phishing scams operating daily. One such scam installed 12 different pieces of malware and resulted in the theft of at least 60,000 Social Security Numbers.

Significantly, Cyveillance reports that smaller regional banks, credit unions, and retail sites are the latest targets of phishing scams. For example, credit unions saw an increase of 584 percent in phishing scams in the last 12 months, and associations have experienced an increase of 329 percent according to the Cyveillance report.

Nonetheless, well-known banks continue to be the main targets. McAfee released a list of the ten most commonly used phishing email subject lines used in March 2007 as to guide for consumers to avoid such scams. Notably, all of the scams involved a reference to a bank. BB&T was the most widely used company name.

An article discussing the Cyveillance report is available at: http://www.darkreading.com/document.asp?doc_id=120373&WT.svl=news1_3

An article with the McAfee list of subject lines is available at: <http://www.pcadvisor.co.uk/news/index.cfm?newsid=8822>



IV. CONSUMER PROTECTION

- **Age Verification on Social Networking Websites Discussed** – A March 23, 2007, discussion sponsored by the Progress and Freedom Foundation addressed the value and feasibility of online age verification technologies, specifically in the context of social networking websites such as MySpace and Facebook. Legislation aimed at protecting children on social networking websites is currently pending in Congress and in several states; some of this legislation calls for age verification. Security experts argued that age verification of children is not feasible due to the lack of records against which to verify their age. A law enforcement representative and a representative of an age-authentication software company stated that parental validation of a child's age is possible. However, other experts countered that this would not be effective and is too easy to get around. This debate is likely to continue as both federal and state legislation in this area moves forward.

An article on this issue is available at:
<http://www.cnsnews.com/news/viewstory.asp?Page=/Culture/archive/200703/CUL20070326a.html>.

V. STATE ISSUES

- **Michigan, Montana, and New Mexico Pass Credit Freeze Legislation** – The Michigan House of Representatives passed legislation on March 20, 2007 that would allow a consumer to place a freeze on disclosure of consumer credit information held by credit reporting agencies within five days of request. A fee, not to exceed \$20, is waived for victims of identity theft. The bill passed the House by a vote of 105-0 and moves to the State Senate for consideration.

The Montana Senate also passed legislation allowing consumers to freeze their credit. The legislation requires credit reporting agencies to freeze the credit of victims of identity theft within 24 hours of notification for free. Other consumers will be required to submit a fee of three dollars. The legislation, Senate Bill 116, passed the Montana Senate 49-0 and awaits the signature of Montana Governor Brian Schweitzer.

The New Mexico legislature also passed security freeze legislation. Senate Bill 165, as passed, would allow consumers to block credit reporting agency disclosure of the consumer's credit information upon written request to the agency. The legislation includes an exemption for the underwriting of insurance.

Text of Michigan House Bill 4103 as passed by the Michigan House of Representatives is available at: <http://www.legislature.mi.gov/documents/2007-2008/billengrossed/House/htm/2007-HEBH-4103.htm>.

Text of Montana Senate Bill 116 as presented to the Governor is available at: <http://data.opi.mt.gov/bills/2007/billhtml/SB0116.htm>.



Links to the text of New Mexico Senate Bill 165, proposed amendments to it, and various analyses of the legislation are available at:

http://legis.state.nm.us/lcs/_session.asp?chamber=S&type=++&number=165&Submit=Search&year=07.

- **Texas Social Security Number Legislation Awaits Governor's Signature** – The Texas legislature passed legislation on March 19, 2007 that would require government officials to redact all but the last four digits of a citizen's social security number on public documents upon written request. However the bill also declares that social security numbers are not confidential information, which otherwise would require the redaction of social security numbers from all public documents under the Texas Public Information Act according to an earlier opinion by Texas Attorney General Greg Abbott. The bill would allow district and county clerks to disclose social security numbers in the ordinary course of business.

Links to the Text of the legislation and various state analyses are available at:
<http://www.capitol.state.tx.us/BillLookup/Text.aspx?LegSess=80R&Bill=HB2061>.

April 4, 2007 – April 16, 2007.

I. PRIVACY

- **Jury Award for Misleading Opt-Out Upheld** – Judge Anna J. Brown of the U.S. District Court for the District of Oregon recently upheld a jury's \$4.5 million award in a Lanham Act litigation between two online college application programs. This litigation has been reported on in previous issues of the *Privacy and Data Security Briefing*.

The dispute had centered on XAP's promise in its privacy policy that personal data entered by the user would not be shared with third parties without the user's express consent. XAP then sold the information of students who responded affirmatively when asked if they were interested in receiving information about student loans or financial aid. The district court initially allowed CollegeNET to proceed with an unfair competition claim based on the finding that XAP's opt-in question was vaguely worded and might not constitute express consent. The jury found the statement to be unfairly competitive in violation of the Lanham Act and awarded CollegeNET damages of \$4.5 million.

Judge Brown upheld the jury's award, finding it to be a reasonable assessment of actual damages. Judge Brown declined to award CollegeNET any of XAP's profits or to increase the damages award as CollegeNET sought. She did grant CollegeNET attorneys' fees based on the finding that XAP engaged in willfully deceptive misconduct, stating, "[t]he only reasonable inference and conclusion to be drawn from this record is that XAP used its privacy policy statements to mislead students and to give them a false sense of security that their personal information would remain private."



This case highlights the importance of privacy policies and ensuring that data collection and use practices match statements made in privacy policies. Additionally, the case illustrates the importance of obtaining informed express consent if necessary.

The decision in this case is available at: http://corp.collegenet.com/news/court_order_3-26-07.pdf.

CollegeNET's press release is available at: <http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/03-27-2007/0004554527&EDATE>.

An article on this case is available at: <http://www.pr-inside.com/judge-rejects-collegenet-inc-s-attempt-r77154.htm>.

- **Prima Facie Evidence of Harm Required Before Identity of Online Posters Will Be Revealed** – The Court of Common Pleas of Allegheny County, Pennsylvania has held that in order to balance state libel laws with the First Amendment right of online speakers to speak anonymously, a plaintiff must submit prima facie evidence that statements were unlawful in order to compel discovery of an online poster's identity. In the case at issue, a corporation alleged that three online posters had defamed the corporation through Yahoo's financial chat pages. The court held that the plaintiff corporation would have to show prima facie evidence that the statements were false, that the posters intended to cause pecuniary loss, and that pecuniary loss did occur before the court would reveal the identity of the anonymous posters. This decision may also be viewed as upholding the individual's right to privacy online.

The court's decision in this case is available at: http://palawlibrary.com/sample_case1.pdf.

II. SECURITY

- **Forrester Research Releases Study on the Cost of Data Breaches** – A report by Forrester Research found that the cost of data breaches varies widely from \$90 to \$305 per lost record. The report is based on surveys with 28 companies that have experienced data breaches. These costs include the expense of remediating the breach, notifying customers, regulatory and legal compliance, and lost productivity. These estimates are within the range that other research entities have projected, but may not fully take into consideration the other non-monetary losses associated with breaches.

A copy of the report can be purchase at: <http://www.forrester.com/Research/Document/Excerpt/0,7211,42082,00.html>.



III. SPYWARE

- **FTC Asks Congress for More Resources to Combat Spyware and Other Unlawful Activities** – During recent testimony by FTC Chairman Deborah Platt Majoras, and fellow Commissioners Harbour, Leibowitz, Kovacic, and Rosch, the FTC asked Congress for more tools and broader power to challenge anti-fraud activities, including spyware and other technology fraud issues. Included in their request was an increase of \$17 million from the FTC's FY 2007 budget request. The funds would be used for a variety of FTC activities, including \$100,000 that would be used to increase enforcement efforts to combat spyware. Although a nominal amount in comparison to the funding request, spyware was repeatedly mentioned as an area of focus for the FTC; in its testimony, the FTC highlighted the fact that they have brought eleven spyware enforcement actions in the past two years (specifically mentioning the *Direct Revenue* case). The FTC also stated that they will continue to bring cases in this area.

In making their request for stronger legislation to empower their fraud fighting efforts, the FTC also asked for more civil penalty authority in the area of data security, telephone pretexting, and spyware. Chairman Majoras said the FTC would be more effective if it had the authority to seek punitive damages and noted that legislation in all of these areas is pending in Congress, which the FTC supports. Currently, the FTC is able to seek punitive damages when a breach involves a violation of the Fair Credit Reporting Act, which was the case in the FTC's action against ChoicePoint. In that case, the FTC secured \$5 million in consumer redress and \$10 million in civil penalties from the company.

The FTC's testimony is available at: <http://ftc.gov/os/testimony/P040101FY2008BudgetandOngoingConsumerProtectionandCompetitionProgramsTestimonySenate04102007.pdf>.

IV. SPAM

- **New Report Notes Impact of Rise in Spam on Marketers** – Numerous reports have documented the notable rise in spam in recent months. A recent report released by the E-Mail Sender and Provider Coalition (ESPC) in conjunction with market research firm Ipsos highlights the implications of this increase in spam for legitimate email marketers. According to the report, more than 80 percent of the 2,200 online users surveyed said they report spam or use unsubscribe options. Notably these respondents also said that they do not even open an email prior to using the "Report Spam" button. Consequently, the ESPC report suggested that senders include identifying information in the "From" and the "Subject" lines of emails. ESPC also suggests displaying a certified icon in the email.

A summary of the report is available at <http://www.espccoalition.org/032707consumer.php>.



- **New Technology Designed to Stop Spam** – Canadian company, MailChannels, has introduced a new product called Traffic Control to combat spam. Through company research, MailChannels found that spammers will stop trying to send email if they are forced to wait even a few seconds before they can communicate with Internet servers handling incoming email. The company's research suggests that a ten second delay forces as many as 90 percent of spammers to abandon efforts to send their message whereas legitimate email senders will continue to try to deliver their message. In response to these findings, MailChannels created Traffic Control, as software that will allow administrators to extend the traditional two second communication gap from 10 seconds to a couple of minutes so as to stop the influx of spam. As spam continues to proliferate, it is likely that new technologies such as Traffic Control will continue to be developed to thwart the problem.

An article about this development is available at: <http://www.washingtonpost.com/wp-dyn/content/article/2007/04/10/AR2007041000479.html?hpid=moreheadlines>.

V. TELECOM/WIRELESS

- **FCC Releases Text of CPNI Order** – On April 20, 2007, the FCC released the text of its CPNI Order, which revised substantially the regulations applicable to the use and sharing of call data. The most significant – and controversial – changes to the FCC's rules pertain to customer password authentication requirements, data breach disclosure obligations, and a new "opt-in" rule for sharing call data with third parties. Under the new customer password authentication requirements, carriers are prohibited from releasing the most sensitive category of call data (call detail information) during customer-initiated telephone contact unless the customer provides a password. Absent a password, the data only can be sent to the customer address of record or disclosed if the carrier calls back the customer at the telephone number of record. Under the new data breach disclosure obligations, carriers must notify customers if the security of their call data has been compromised, but not before contacting and providing law enforcement officials with the opportunity to prevent such disclosure (which could occur if, for example, the "breach" was caused by a law enforcement request for the data). Under the new "opt-in" rule, carriers may not share call data with joint venture partners and independent contractors absent the customer's express agreement to have that data shared. The FCC's rules previously required carriers to provide customers with only an "opt-out." The new rules dramatically shift the balance that previously existed between carriers and customers with respect to control over call data, and it has been widely reported that an appeal of the new rules is likely.

A copy of the FCC's CPNI Order can be found at:
http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.doc.

- **House Passes Anti-Spoofing Measure** – On March 22, 2007, the House passed H.R. 740, the "Preventing Harassment through Outbound Number Enforcement Act of



2007," which would make it illegal to falsify caller ID information with the intent to defraud. The House Commerce Committee on March 15, 2007 approved H.R. 251, known as the "Truth in Caller ID Act," but it is rumored to not be moved forward any farther because it lacks a law enforcement exception. A similar measure was passed by the House in the last Congress, but the Senate never acted on it. It remains unclear whether the Senate will act on the issue in this Congress, although similar measures have been introduced there.

Additional information about H.R. 740 and H.R. 251 can be found at:
<http://thomas.loc.gov/cgi-bin/query/D?c110:4:./temp/~c110Au22Iz> and
<http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.00251>.

VI. CONSUMER PROTECTION

- **Darden Restaurants Settles with FTC Regarding Gift Card Practices** – The FTC announced on April 3 that Darden Restaurants, which owns restaurant chains Olive Garden, Red Lobster, Smokey Bones, and Bahama Breeze, agreed to settle charges that it had engaged in deceptive practices in the marketing and sale of its gift cards. This is the FTC's second action involving gift cards, following its recent announcement of a settlement with Kmart (reported in a previous issue of the *Privacy and Data Security Briefing*). According to the FTC's complaint, Darden did not adequately disclose that dormancy fees of \$1.50 per month would be assessed after 15 or 24 months of non-use (depending on whether the card was purchased before or after February 2004). The FTC further alleged that the disclosures on the card itself were inadequate – they appeared in fine print on the back of the card and were allegedly obscured by other miscellaneous information. Additionally, consumers who purchased gift cards online were allegedly not provided pre-sale disclosures.

As of October 2006, Darden stopped charging the dormancy fee on its gift cards. The settlement requires Darden to restore the dormancy fees to any affected cards and to publicize the restoration program on its websites for two years. Darden has already completed the automatic restoration process. In the future, Darden must clearly and prominently disclose any expiration date and potential fees in any advertising, at point of sale, and on the front of all gift cards.

The FTC's interest in the area of gift cards, as evidenced by the Darden and recent Kmart settlements, indicates that retailers must take care to clearly and prominently disclose to consumers key information concerning gift cards, including any potential fees and restrictions.

The FTC's press release and related documents are available at:
<http://ftc.gov/opa/2007/04/darden.htm>.



VII. STATES

- **Texas Attorney General Files Complaint Against Radio Shack for Improper Disposal of Customer Records** – Texas Attorney General Greg Abbott has filed a complaint against Fort Worth-based Radio Shack Corporation for exposing its customers to identity theft when employees dumped customer records in bulk using garbage containers behind a Radio Shack store. Investigators report that these records contained sensitive consumer information, including Social Security numbers, credit and debit card information, names, addresses, and telephone numbers. According to the Attorney General's complaint, this action violated a 2005 law requiring businesses to protect any consumer records that contain sensitive information.

This lawsuit serves as a warning to companies to take precautions at all levels of the company to dispose of hard copy, as well as electronic, documents in a secure manner and without violating applicable laws. In addition to Texas, California, Arkansas, and Nevada have laws mandating "reasonable security measures" for databases containing consumer records.

A copy of the Texas Attorney General's complaint and related press release is available at: <http://www.oag.state.tx.us/oagNews/release.php?id=1961>

- **New Washington Law to Address Identity Theft** – The Washington legislature passed a law that would enable Washington residents to freeze unauthorized access to their credit reports. The legislation is scheduled to be delivered to the Washington Governor for his signature.

By amending Washington's Fair Credit Reporting Act, SSB 5826 makes available a credit freeze that allows Washington consumers to prevent a consumer's credit file from being shared with potential creditors. This is designed to prevent identity theft because businesses generally will not create credit accounts without first examining a consumer's credit history. The law also provides a mechanism that would allow consumers to authorize temporary, restricted access to their credit files. Identity theft victims and seniors ages 65 and older will have free access to the credit freeze while other consumers will pay to up \$10 to each bureau for their freeze, a temporary lift, or removal.

An article about the new law is available at: <http://www.insurancejournal.com/news/west/2007/04/09/78560.htm>.

- **California and Arizona Remove Social Security Numbers From Public Documents** – Amid increasing calls to protect disclosure of private information in public documents, the California Secretary of State, which serves as the central filing office for certain financing statements and lien documents, has temporarily shut down portions of the Uniform Commercial Code (UCC) website because some publicly available documents displayed individuals' Social Security numbers. Under current law, some UCC documents are available to anyone who requests and pays for a copy of them. However,



the Secretary of State has indicated that the documents will remain blocked until consumers' Social Security numbers are removed from the publicly available records.

Relatedly, the Arizona House has approved a bill that would require Maricopa county recorders to prevent people who access public documents on the Internet from obtaining Social Security numbers appearing on these documents. Other counties in Arizona have the option of instituting similar protections but would be required to honor individual request to redact their Social Security numbers from Internet accessible documents. Social Security numbers would be still accessible at the county offices as required by law. The bill has already been approved by the Arizona Senate.

An article about the California Secretary of State's action is available at: http://www.govtech.net/magazine/channel_story.php/104602.

An article about the recently passed Arizona law is available at: <http://www.eastvalleytribune.com/story/87687>.

VIII. RADIO FREQUENCY IDENTIFICATION TECHNOLOGIES (RFID)

- **California State Senate Considers Five Bills on RFID** – California State Senator Joseph Simitian has sponsored bills seeking to regulate the use of RFID with driver's licenses or identification cards, for tracking public school students, for government-issued IDs, to make the intentional unauthorized remote reading of another person's identification document a misdemeanor crime, and to prohibit the subcutaneous implanting of an identification device. Specifically,
 - SB 28 would prohibit, until January 1, 2011, the Department of Motor Vehicles from issuing, renewing, duplicating, or replacing a driver's license or identification card, if the license or card uses radio waves to either transmit personal information remotely or to enable personal information to be read from the license or card remotely. Although the bill is set for a vote, the Senate has not yet done so as of April 16, 2007.
 - SB 29 would prohibit, until January 1, 2011, a public school, school district, and county office of education from issuing any device to a pupil that uses radio waves to transmit personal information or to enable personal information to be viewed remotely for the purposes of tracking the location of a pupil on school grounds, or both. Although the bill is set for a vote, the Senate has not yet done so as of April 16, 2007.
 - SB 30 would enact the Identity Information Protection Act, which would create interim privacy safeguards for existing RFID-enabled government IDs. The Senate Committee on Public Safety has scheduled a hearing regarding this bill to be held on April 24, 2007.



- o SB 31 would make it a misdemeanor crime for a person or entity to intentionally remotely read or attempt to remotely read a person's identification document using radio waves without his or her knowledge and prior consent. The new crime would be punishable by imprisonment in a county jail for up to one year, a fine of not more than \$5,000, or both that fine and imprisonment. The Senate Committee on Public Safety has scheduled a hearing for this bill to be held on April 24, 2007.
- o SB 362 would prohibit a person from requiring, coercing, or compelling any other individual to undergo the subcutaneous implanting of an identification device. Among other things, the bill would provide specified rights of action and remedies for violations of its provisions. The Committee on Appropriations has scheduled a hearing for this bill to be held on April 23, 2007.

Senator Simitian introduced legislation identical or similar to the above bills last year, but was unsuccessful in getting any of the bills passed. Governor Schwarzenegger vetoed RFID legislation last year, but he reportedly has not taken a position on the new bills mentioned above.

A copy of SB 28, and related information, can be found at http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_28&sess=CUR&house=B&author=simitian.

A copy of SB 29, and related information, can be found at http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_29&sess=CUR&house=B&author=simitian.

A copy of SB 30, and related information, can be found at http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_30&sess=CUR&house=B&author=simitian.

A copy of SB 31, and related information, can be found at http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_31&sess=CUR&house=B&author=simitian.

A copy of SB 362, and related information, can be found at http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_362&sess=CUR&house=B&author=simitian.

An article discussing these bills can be found at http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleID=288107&intsrc=news_ts_head.



April 16, 2007 – May 4, 2007.

I. PRIVACY

- **Consumer Groups Object to Google's Proposed Acquisition of DoubleClick** – The Electronic Privacy Information Center, along with the Center for Digital Democracy and the U.S. Public Interest Research Group, filed a complaint with the Federal Trade Commission (FTC) on April 20, 2007 requesting that the FTC block Google's acquisition of DoubleClick until the FTC investigates the privacy implications of the deal. Microsoft had previously asked the government to consider the antitrust and privacy issues involved in combining the two entities.

Google is the largest search engine in the U.S., and DoubleClick is the country's largest ad technology provider. The public-interest groups voiced concerns about the possibility of combining the search histories of Google users with online surfing behavior collected by DoubleClick cookies to create a detailed picture of a consumer's online behavior. The groups argue that the large amount of data collected will make Google vulnerable to security breaches and law enforcement surveillance requests. The complaint asks that the FTC order Google to create a "meaningful data destruction policy," and to provide users reasonable access to information stored about them.

Google CEO Eric Schmidt stated that Google is working on technology to handle cookies that would reduce concerns, although he did not provide details. He also promised changes in the company's policies, emphasizing that Google would do whatever was necessary to satisfy privacy concerns. He further noted the potential benefits of a greater use of personal data collected online – from allowing for more personalized services to fighting terrorism. Google has also stated that for now it does not plan to merge personally identifiable information with Internet-surfing behavior, but that it would combine non-personally identifiable data (search histories and surfing behavior linked to an IP address) in order to better target advertisements. The complaint to the FTC, however, notes that with some effort an IP address may be linked to an individual.

We will continue to monitor its privacy implications and their potential effects on the online advertising industry.

Articles on this issue are available at: <http://www.washingtonpost.com/wp-dyn/content/article/2007/04/21/AR2007042100085.html>; http://news.com.com/Google+draws+privacy+complaint+to+FTC/2100-1024_3-6177819.html?tag=item; and <http://www.ft.com/cms/s/284f2b08-f104-11db-838b-000b5df10621.html>.

The complaint to the FTC is available at: <http://www.ft.com/cms/s/284f2b08-f104-11db-838b-000b5df10621.html>.



- **Google Plans to Strengthen Privacy Warnings on Google Calendar-**

Google is working on improving the messaging about privacy settings on Google Calendar, although the company is not certain when the changes will be implemented. Google Calendar is a web-based application that allows users to store event, contact, and other data online and access the data from anywhere. By default, such information is private, but users may choose to disable the default setting and make such information public. When users make this choice, Google takes steps to ensure that they are aware that they have made the settings public – the screen goes grey, and the user must acknowledge awareness of the change. However, it appears that users may forget that they made this change. A search using Google Calendar's public search feature revealed some highly personal information, including usernames and passwords for websites and email accounts, as well as corporate meeting dates and dial-in information for internal calls. Google's changes would be an attempt to remind consumers that the default privacy settings have been changed in order to create a more visible and persistent reminder for consumers.

Google's consumer-friendly efforts raise the question of how much a company should or must do to protect consumers from their own choices, especially when initial disclosures appear to be clear.

An article on this issue is available at:

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9017259>.

- **Pew Study Looks at Teens, Social Networking, and Privacy** - The Pew Internet & American Life Project released its latest study of teens and social networking on April 18, 2007. The study was based on a survey of 935 youths aged 12 to 17. The study found that the majority of teens surveyed take steps to protect their privacy online. Fifty-five percent of teens now have online social networking profiles, and two-thirds say their profile is not visible to all online users. At the same time, the teens do reveal a lot of information, including first name, photos, name of their city/town, and name of their school, among other information. The fact that many teens make their profiles private, or visible only to certain users, is encouraging and may indicate that teens are not as oblivious to privacy concerns as has been often suggested. The study contains a number of additional statistics and observations about online teens.

The Pew press release and a link to the full report are available at:

http://www.pewinternet.org/PPF/r/139/press_release.asp.

II. SECURITY

- **Senate Commerce Committee Approves Data Security Bill** – The Senate Committee on Commerce, Science and Transportation voted to approve S.1178, the Identity Theft Protection Act. As discussed in previous *Privacy and Data Security Briefings*, the bill would require companies to notify customers of data breaches when there was



“reasonable risk of identity theft”, allow consumer to place security freezes and require companies to take basic steps to protect consumer data.

During mark-up, the bill was amended to include a prohibition on buying or selling Social Security numbers. These new provision contained a limited exception for law enforcement or public health purposes. But, if enacted, the provision would likely be interpreted by the Federal Trade Commission to prevent companies from selling marketing lists that include Social Security numbers.

Other amendments accepted during the mark-up included 1) a provision to allow state attorneys general, who can also enforce the Act, to recover costs and attorneys fees and 2) a provision to allow companies that primarily communicate with customers via e-mail to send breach notices via e-mail as well.

A copy of the bill is available at: http://thomas.loc.gov/cgi-bin/t2GPO/http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:s1178is.txt.pdf

- **Identity Theft Task Force Releases Report** – The President's Identity Theft Task Force has released a report titled “Combating Identity Theft – A Strategic Plan”. The report offers a comprehensive set of recommendation that apply to government agencies and the privacy sector. Of particular interest are the following:
 - The report urges Congress to pass a data security bill that would require all companies to adopt basic data security protocols and to notify consumers in the event of a breach. The report recommends preempting state law and allowing federal regulators to seek civil penalties. The report is silent on the role of state attorneys general.
 - The report recommends that federal agencies continue to initiate investigations into potential violations of data security requirements.
 - The report recommends a comprehensive review of the private sector use of Social Security numbers. While the report stops short of recommending restrictions on the use of this data, the information gained by such a review would certainly be used to encourage or discourage several pending bills that address this issue.
 - The report urges all federal agencies that have data security as part of their mandate to assess whether they have sufficient authority to seek civil penalties and, if not, to gain that authority through legislation if necessary.

The report is available from the Task Force's website, at: <http://www.idtheft.gov/>

- **Senate Judiciary Committee Approves Data Security Bill** – The Senate Judiciary Committee approved on a voice vote S.495, the Personal Data Privacy and Security Act. The Committee also rejected a competing measure sponsored by Senator Jeff Sessions (R-AL). Unlike S.1178, discussed above, notice of a breach is required if there is a “significant risk” of harm (not only of identity theft). But the burden is on companies to



show that there is no significant risk and these findings can be overturned by the U.S. Secret Service, which must receive a copy of the company's risk assessment. The bill would also require all companies to adopt basic data security safeguards.

S.495 also includes specific new obligations for data brokers, including a requirement to allow consumers to access their records and provide a mechanism for correcting mistakes. The requirements are loosely modeled on those of the Fair Credit Report Act, which applies to certain services offered by the large credit bureaus and other similar companies, but does not apply to other large and small data brokers. The definition data brokers is broad and includes any company "which for monetary fees or dues regularly engages in the practice of collecting, transmitting or provided access to sensitive personally identifiable information" of people who are not customers or employees of the company. The unqualified inclusion of "transmission" at least raises the possibility that these regulations could be applied indiscriminately to back-office functionalities that are generally not considered the target of such legislation.

The Committee also approved S.239, which contains the same breach notification requirements as Title III, subtitle B of S.495. The approval of both bills allows breach notification to move forward even if the broader measure is held up by either jurisdictional fights or lobbying by data brokers, many of whom are opposed to the additional obligations in S.495.

III. SPYWARE

- **House Judiciary Committee Subcommittee Approves "I-Spy" Anti-Spyware Bill** – The "Internet Spyware (I-SPY) Prevention Act of 2007," which is nearly identical to legislation that passed the full House 395-1 in the 109th Congress but failed to garner Senate approval, is sponsored by Reps. Zoe Lofgren (D-CA) and Bob Goodlatte (R-VA) and will now go to the full House Judiciary Committee for consideration. The bill aims to combat spyware and phishing schemes that attempt to trick consumers into revealing personal financial information. The legislation provides for fines and imprisonment up to five years for persons that intentionally accesses a users' computer without authorization or in excess of user authorization by downloading a computer program onto that computer for the purpose of defrauding the user or to further another criminal offense.

Information from the Library of Congress' Thomas website regarding HR 1525 is available at: <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.01525>:

- **House Subcommittee on Commerce, Trade and Consumer Protection Approves "Spy Act"** – Not to be outdone by efforts in the House Judiciary Committee, the Commerce, Trade and Consumer Protection Subcommittee passed its own anti-spyware legislation. The bill, HR 964, is sponsored by Edolphus Towns (D-NY) and Mary Bono (R-CA), and is similar to measures passed by the full House in the last two Congresses. H.R. 964, the "Securely Protect Yourself Against Cyber Trespass Act" or "Spy Act," would require companies to provide adequate notice and obtain consent from users before



downloading their software onto consumers' computers. The legislation would also require that such software be easily removable and would also give the FTC the ability to impose greater penalties on violators.

Information from the Library of Congress' Thomas website regarding HR 964 is available at: <http://thomas.loc.gov/cgi-bin/query/D?c110:1:./temp/~c110rK4BCg:> .

IV. SPAM

- **FTC Spam Summit Announced** – The FTC set a date for a two-day public event, "Spam Summit: The Next Generation of Threats and Solutions." The summit will be held in Washington, DC on July 11 and 12, 2007. According to the FTC announcement, the event will bring together noted experts from the private sector and government to consider consumer protection issues raised by spam, phishing, and malware. Although the final agenda has not been set, the FTC expects to address the following topics:
 - defining today's spam problem;
 - new methods for sending spam;
 - economic incentives for sending spam;
 - challenges to effective deterrence;
 - emerging spam threats in other media;
 - technological tools to fight spam; and
 - stakeholder best practices in reducing malicious spam.

The FTC is soliciting written comments on the topics to be addressed at the summit. Any such comments must be submitted by May 18, 2007. Hogan & Hartson, LLP will attend the summit and report on any developments in subsequent issues of the *Privacy and Data Security Briefing*.

An FTC release announcing the summit is available at: <http://www.ftc.gov/bcp/workshops/spamsummit/index.shtml>.

- **Spam Class Action Filed** – Project Honey Pot, an organization that offers a free anti-spam service that collects information on e-mail address harvesters, has filed an anti-spam-related class action under Virginia's anti-spam statute and CAN-SPAM law in the U.S. District Court in Alexandria, Virginia. The complaint was filed on behalf of approximately 20,000 Internet users in more than 100 countries.

Webmasters that installed Project Honey Pot's software on their servers enabled the organization to collect information on individuals or bots that scan websites for e-mail addresses and then store them in a database for sale to spammers. Project Honey Pot hopes that this information along with subpoenas filed in connection with its lawsuit will enable the organization to determine the identity of actual spammers.



If successful, the lawsuit purportedly could entitle the company more than \$1 billion in statutory damages against spammers.

An article about this development is available at:

<http://arstechnica.com/news.ars/post/20070426-project-honey-pot-springs-1-billion-lawsuit-on-spammers.html>.

A copy of the Project Honey Pot complaint is available at:

http://www.projecthoneypot.org/downloads/ProjectHoneyPot_Stamped_Complaint_4_26_07.pdf.

- **Newsletter Spam Is Latest Spamming Technique** – Spammers continue to find new ways to avoid filters and attack consumer inboxes. The latest reported trend is hijacked newsletter spam. According to anti-spam firm Commtouch, newsletter spam avoids anti-spam filters by using dressing their mail up as popular e-mail newsletters and inserting a spam image at the beginning of the message. Commtouch also confirms the widely reported increase in spam with its findings that 85 percent to 90 percent of all e-mail is spam.

An article highlighting the Commtouch report is available at:

<http://www.dmnews.com/cms/dm-news/e-mail-marketing/40857.html>.

The Commtouch report is available at:

http://www.commtouch.com/downloads/Commtouch_2007_Q1_Spam_Trends.pdf

V. TELECOM/WIRELESS

- **DOJ FISA Revisions Would Protect Phone Companies; Senate Intelligence Committee to Assess Phone Company Immunity at Upcoming Hearing** – On April 13, 2007, officials at the U.S. Department of Justice began circulating proposed amendments to the Foreign Intelligence Surveillance Act which would, among other things, grant telephone companies civil immunity from privacy-related lawsuits if they cooperate with law enforcement anti-terrorism efforts under FISA. The extent to which such companies are liable for responding to law enforcement requests for consumer telephone data currently is unclear. The Senate Intelligence Committee is scheduled to consider the DOJ's proposed revisions to FISA at a hearing on May 1, 2007.
- **AT&T Announces Pretexting Settlement With Data Brokers** – On April 17, 2007, AT&T announced that is entered into settlement agreements with more than a dozen data brokers accused of using fraudulent practices to obtain consumer telephone records. The settlements were with data brokers operating in California and Texas, only one of whom (Lobel Financial Corporation) has not yet agreed to settle claims made by AT&T.

Additional information about this development can be found at:

<http://setup2.wsj.com/article/SB117683948906273002.html>.



- **Senate Judiciary Committee Approves Anti-Spoofing Measure** – On April 25, 2007, the Senate Judiciary Committee approved by voice vote H.R. 740, a bill previously passed by the House on March 21, 2007, that would make it a criminal offense to transmit false caller identification information with the intent to defraud. The draft of the bill passed by the Senate Judiciary Committee included an amendment introduced by Senator Leahy (D-VT) clarifying that the measure protects businesses as well as individuals. Although a number of other anti-spoofing measures have been introduced in both houses of Congress, H.R. 740 now appears to be the frontrunner for passage in this Congressional term.

Additional information about H.R. 740 can be found at: <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:HR00740:@@L&summ2=m&>.

VI. STATES

- **Challenge to Utah Trademark Protection Act Likely** – Google is engaged an effort to educate lawmakers about potential constitutional problems raised by the recently adopted Utah Trademark Protection Act. The Utah law, which is currently slated to take effect on June 30, allows companies to apply for an “electronic register mark” for their trademarked brands. Once registered, the brands would be identified in a state database. These registered marks would be protected from competitors that want to purchase the right to use those brands to show ads linking to their own sites. Therefore, under the law, if a consumer located in Utah types a trademarked brand into a search engine, and a competitor serves a sponsored ad for their site, the owner of the trademarked brand could sue the search engine and the competitor.

While currently the focus of much national debate on policy and copyright issues, the law was passed with little opposition earlier this year. Nonetheless, a legal challenge was acknowledged in a legislative review note that indicated that the law had could be found unconstitutional and a legal challenge was reportedly expected even by proponents of the legislation. Google has made public statements that the law violates free speech and is inconsistent with U.S. trademark law.

An article about this development is available at: http://www.sltrib.com/ci_5639856.

A copy of the bill is available at: <http://le.utah.gov/~2007/bills/sbillamd/sb0236.htm>.

- **Nebraska Bill Would Restrict Use of Social Security Numbers** – Nebraska state legislators gave first round approval in favor of LB 674, a bill that would limit employer use of employees' Social Security numbers (SSNs). If ultimately adopted after a second round of debate and voting, the bill would prohibit employers from:
 - requiring workers to use SSNs to access Internet sites;
 - sending SSNs via unencrypted e-mail;



- o using an individual's full SSN as an employee identification number;
- o publicly posting employees' SSNs or allowing the public or co-workers to access SSNs, including by leaving SSNs in unsecured files; and
- o allowing temporary workers access to files containing SSNs, unless those temporary workers were bonded or otherwise insured.

A violation of these provisions would be considered a misdemeanor, punishable by a \$100 fine.

The Nebraska law is exemplary of the trend in many states to discourage widespread use of SSNs as an identifier.

An article about this development is available at:

http://www.omaha.com/index.php?u_page=2798&u_sid=2367391.

A copy of the bill is available at:

<http://uniweb.legislature.ne.gov/FloorDocs/Current/PDF/Final/LB674.pdf>.

- **Texas AG Files Another Lawsuit Relating to Discarded Consumer Records** – Texas Attorney General Greg Abbott filed a lawsuit against CVS Corporation after CVS pharmacy employees allegedly threw away credit card numbers, medical information, and other sensitive material from more than 1,000 customers into a garbage container while a CVS store was being vacated. This lawsuit comes only a few weeks after Attorney General Abbott filed a similar suit against Radio Shack (as reported on in the last edition of the *Privacy and Data Security Briefing*).

In the most recent lawsuit, CVS is charged with violations of the Texas Identity Theft Enforcement and Protection Act, which requires the protection and proper destruction of clients' sensitive personal information, as well as violations of Chapter 35 of the Business and Commerce Code, which requires businesses to develop retention and disposal procedures for their clients' personal information.

The Texas Attorney General's activity in this area is a continued reminder to all companies to develop and abide by data destruction procedures that protect consumers' personal information.

An article about this development is available at:

http://biz.yahoo.com/ap/070417/tx_cvs_identity_theft.html?.v=1&printer=1.

A copy of the complaint is available at:

http://www.oag.state.tx.us/newspubs/releases/2007/041607cvs_pop.pdf.



VII. RADIO FREQUENCY IDENTIFICATION TECHNOLOGIES (RFID)

- **Pennsylvania and New Hampshire introduce RFID legislation** – Pennsylvania and New Hampshire are the latest states to introduce legislation that would seek to regulate, and in some instances prohibit, the use of RFID technologies. Specifically,
 - o Pennsylvania H.B. 992 would criminalize the unauthorized remote reading of personal information using RFID technology, in which a microchip emits radio signals that are picked up by a reader.
 - o Pennsylvania H.B. 993 seeks to regulate the use of RFID tags under Pennsylvania's Unfair Trade Practices and Consumer Protection Law by requiring business to provide notice to consumers if their products contain RFID tags, to alert them if RFID readers are in use in a public area, and to attach tags in a manner that allows consumers to remove them after the object has been purchased or issued without damaging the object. The bill would permit consumers to file complaints alleging violations of the law with the Bureau of Consumer Protection in the Office of the Attorney General.
 - o New Hampshire H.B. 686 would regulate the use of RFID in consumer products, except, for example, in cell phones, WiFi cards, and GPS receivers, by requiring labels that inform consumers of their presence. The bill would also restrict the circumstances under which the State may use electronic tracking devices and prohibits private citizens from electronically tracking another person without the person's consent. The bill also prohibits the implantation of RFID in human beings without the informed, written consent of the individual or their legal guardian. The legislation would assign criminal and civil liability to violations of the law.

The Pennsylvania bills can be found at:

<http://www.legis.state.pa.us/cfdocs/billinfo/billinfo.cfm?year=2007&sind=0&body=H&type=B&BN=0992>;

<http://www.legis.state.pa.us/cfdocs/billinfo/billinfo.cfm?year=2007&sind=0&body=H&type=B&BN=0993>.

The New Hampshire bill and an article discussing it can be found at:

<http://www.gencourt.state.nh.us/legislation/2007/HB0686.html> and

<http://www.heartland.org/Article.cfm?artId=21011>.



May 8, 2007 – May 22, 2007.

I. PRIVACY

- **Google Files Patent Regarding In-Game Advertising** – Google has filed a patent in Europe and the U.S. describing how the online behavior of individuals who play online games such as Second Life and World of Warcraft could be used to send more targeted in-game advertisements to those individuals. For example, user dialogue and user play could be used to characterize the user so that ads targeted to that type of user could be sent. Privacy advocates have expressed concern about the implications of compiling and storing such detailed information. The proposed profiling techniques would require games publishers to actively incorporate Google's technology. Google has stated that it does not have plans to roll out the technology in the near future. In-game advertising appears to be a growth area that will likely continue to raise privacy questions.

An article on this development is available at:

<http://technology.guardian.co.uk/news/story/0,,2078061,00.html>.

- **IRS Seeks Personal Data from Websites** – President Bush's 2008 budget contains a proposal that would require online "brokers" such as eBay and Amazon.com to file income statements with the IRS for all customers who use their sites to conduct 100 or more separate transactions that generate \$5000 or more per year. Such online brokers would be required to collect customers' names, addresses, and taxpayer identification numbers or Social Security numbers. Although the provision appears to be limited to certain high-volume customers, in practice, the online brokers would likely collect information from all of their customers in order to insure compliance; it is the online broker that would be held liable under the proposal. The Center for Democracy and Technology has warned that this proposal could lead to the collection of Social Security numbers and other personal information by many different online entities, which in turn generates concerns about government and wrongdoer access to such data. The proposal and accompanying data security requirements would also likely be costly for businesses. We will continue to monitor the progress of this proposal.

An article on this issue is available at:

http://www.cio.com/article/108405/IRS_Wants_Data_on_Users_from_Web_Firms.

The Center for Democracy and Technology's analysis of this proposal is available at:

<http://www.cdt.org/publications/policyposts/2007/07>.

- **Online Advertising Company Buyouts Continue** – Recently announced proposed acquisitions of online advertising companies include Microsoft's acquisition of aQuantive, Google's acquisition of DoubleClick, Yahoo's acquisition of Right Media, and the WPP Group's acquisition of 24/7 Real Media. While privacy concerns are often mentioned in the discussion of these deals, the objections are largely based on a false premise – that the acquirer will have access to more personally identifiable information post acquisition. These concerns are neither well founded nor subject to antitrust review, and we doubt that the government will review data practices in the course of antitrust approval.

- 77 -

\\DC - 073009\000300 - 2592236 v1



- **National Research Council Calls for National Privacy Commissioner** – The National Research Council (part of the congressionally-founded National Academies of Science) recently released a report on privacy in the U.S. Among the report's recommendations are the establishment of a national privacy commissioner and the undertaking of a systematic review of current national privacy laws and regulations with the goal of achieving a uniform national standard. The report also specifically recommends that entities collecting personal information be required to obtain meaningful consent.

Currently, U.S. privacy policy enforcement generally is handled by the Federal Trade Commission; the creation of a national privacy commissioner would be more similar to the European models of Germany, Austria, France, and the U.K., for example. It remains to be seen how Congress and the administration will respond to the report's recommendations.

An article on this issue is available at: <http://arstechnica.com/news.ars/post/20070507-national-research-council-calls-for-federal-privacy-czar.html>.

An Executive Summary of the report is available at:

http://books.nap.edu/execsumm_pdf/11896.pdf.

II. SECURITY

- **House Commerce Committee Approves Bill to Restrict Sale of Social Security Numbers** – The House Energy and Commerce Committee approved on a voice vote H.R. 948, which would prohibit the purchase and sale of Social Security numbers, except in limited circumstances. The bill would require the Federal Trade Commission to issue regulations detailing the restrictions and would preempt state laws on the same subject. Violations would be punishable by an \$11,000 fine.

Amendments adopted during the mark-up would prohibit displaying Social Security numbers on the Internet and prohibit anyone from requiring consumers to use their numbers as passwords.

Similar provisions were passed by the Senate as part of S. 1178, a broader data security measure. See the May 7, 2007 *Privacy and Data Security Briefing* for a more in-depth review of S.1178.

A copy of H.R. 948 is available at: http://thomas.loc.gov/cgi-bin/t2GPO/http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h948ih.txt.pdf .

- **Union Sues TSA over Security Breach** – The American Federation of Government Employees has sued the Transportation Security Administration on behalf of TSA employees whose data was on a hard drive lost by the TSA. The suit seeks damages of at least \$1,000 per class member (TSA estimates 100,000 records were lost) and requests TSA be required to:
 - tag and electronically monitor all external hard drives, laptops, and other mobile equipment that stores personal data;
 - encrypt all personal data; and

- 78 -

\\DC - 073009\000300 - 2592236 v1



- o destroy bank account and routing information between six months and one year after the effective date of an employee's termination or resignation.

The suit is brought under the Privacy Act of 1974, which only applies to government agencies and may therefore have limited applicability to private companies.

A press release from AFGE is available at:

<http://www.afge.org/Index.cfm?Page=PressReleases&PressReleaseID=738>.

- **TJX Costs Increase** – In recent securities filings, TJX disclosed that the company has spent \$25 million so far following the theft of more than 45 million credit and debit card numbers. The company also predicted costs will continue to rise both for the investigation and legal proceedings and for upgrades it plans to make to its data security systems. Costs in the second quarter are expected to equal \$0.02 to 0.03 per share.

A copy of TJX's filing is available at:

<http://www.sec.gov/Archives/edgar/data/109198/000115752307005174/0001157523-07-005174-index.htm>.

III. SPYWARE

- **House Passes I-SPY Prevention Act** – The full House passed legislation today by voice vote designed to crack down on malicious spyware by providing criminal penalties. As reported in previous editions of *Privacy and Data Security Briefing*, HR 1525 would allow courts to impose fines or prison sentences up to five years, depending on the offense. The bill would also authorize provision of \$10 million annually to the Justice Department to fight spyware, phishing and other online fraud. Nearly identical versions of the bill have passed in the previous two Congresses but failed to see Senate action.

The text, summary and analyses of HR 1525 are available at the Library of Congress' Thomas Web site at: <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.01525>.

- **House Commerce Committee Approves Spy Act** – An anti-spyware bill that would require notice and consent before personally identifiable information about a user is collected by a Website was approved by the House Energy and Commerce Committee with little debate on May 10, 2007. The approved legislation included a manager's amendment that clarified (and reduced) exemptions for cookies and would require the Federal Trade Commission (FTC) to study and report back to the Committee regarding the bill's prohibitions against collection of personally identifiable information without adequate notice and consent. The amendment also authorizes the FTC to issue regulations modifying the notice and consent requirements of the bill if it finds that consumers have adequate notice of their information's use and exemption or modification of the notice and consent requirements is appropriate and consistent with the public interest.

Text of the legislation and the manager's amendment to it are available at:

http://energycommerce.house.gov/cmtc_mtgs/110-fcmu.051007.hr964.hr948.shtml.

The entire News.com story regarding the Spy Act's markup is available at:

http://news.com.com/House+committee+endorses+SSN+limits%2C+antispayware+effort/2100-7348_3-6182973.html?tag=nefd.top.



IV. SPAM

- **ValueClick Reports FTC Investigation Into Marketing Practices** – In its recent filing with the Securities and Exchange Commission (SEC), ValueClick Inc., an online marketing firm reported that the FTC is investigating some of its marketing practices to determine if the practices violate the CAN-SPAM Act or the FTC Act. The company reported that it received an investigatory letter on May 16, 2007 in which the FTC indicated that it was examining (1) certain ValueClick websites that promise consumers a free gift of substantial value, and (2) the method whereby ValueClick drives traffic to such Websites. The company reported that it intends to fully cooperate with the FTC in connection with this inquiry.

ValueClick has been the subject of commentary that suggested that ValueClick's growth was based on questionable lead generation tactics. In response, ValueClick has maintained that its disclosure and privacy policies comply with applicable state and federal laws.

We will continue to monitor this matter as it develops and report on any other announced investigations into marketing practices.

The company's SEC filing is available at:

http://www.sec.gov/Archives/edgar/data/1080034/000129993307003110/htm_20397.htm

An article about this development is available at:

<http://www.reuters.com/article/governmentFilingsNews/idUSWEN823520070518>.

- **"Spam Fighter" Guilty of Defamation** – In the continuing saga between email advertiser and travel agency, Omega World Travel, and "spam fighter" Mummagraphics Inc. (an Oklahoma City Web design firm), a jury has concluded that Mummagraphics is liable for defamation. See *Omega World Travel v. Mummagraphics Inc.*, E.D. Va., No. 05-cv-00122, 4/27/07.

At issue was Mummagraphics' posting of photos of the advertisers, labeling them spammers. This came after Mummagraphics lost its CAN-SPAM suit against Omega. In response to Internet posting, Omega claimed \$3.8 million in damages.

As reported in an earlier edition of the *Privacy and Data Security Briefing*, defendant Mummagraphics initially brought a CAN-SPAM suit against Cruise.com Inc., a subsidiary of plaintiff Omega World Travel Inc., after receiving email advertisements from the company. The Fourth Circuit dismissed the Mummagraphics CAN-SPAM case after concluding that the complaint did not sufficiently show that the headers in question were misleading, and that CAN-SPAM preempted the alleged state remedies.

In a subsequent trial on the defamation claim, the company presented evidence that it was defamed by online descriptions and images noting that the emails in question had already been deemed not illegal under CAN-SPAM. The jury agreed and awarded Omega \$500,000 in compensatory damages, and punitive damages of \$2,000,000.

This case could serve as a disincentive to plaintiffs seeking to bring potentially frivolous lawsuits under CAN-SPAM against legitimate email advertisers.



An article about this development is available at:
<http://pubs.bna.com/ip/BNA/EIP.NSF/7c407ecc8216ce4185256d05005e8b30/9071f45ff7370f34852572d50077b8c1?OpenDocument>.

V. TELECOM/WIRELESS

- **DOJ Asks FCC to Modify CALEA Standard So More Data Can Be Gathered From Wireless Telephone Taps** – On May 15, 2007, the Department of Justice (DOJ) filed a Petition for Expedited Rulemaking with the Federal Communications Commission (FCC) asking the FCC to modify the technical standard commonly used under CALEA so that law enforcement agencies can gather data transmissions sent by wireless telephones. The modifications sought by the DOJ would include packet activity reporting, time-stamp information, all reasonably available handset location information, and other carrier security, performance and reliability requirements. The DOJ claims that without this additional information, important public safety and national security objectives would be at risk. The Petition is expected to be placed on Public Notice by the FCC and be subject to comment shortly, although a decision on the merits of the Petition is unlikely to be made by the FCC for several months.
- **FCC Fines Mortgage Company \$748,000 for National Do-Not-Call Violations** – On May 14, 2007, the FCC issued an Order of Forfeiture fining Dynasty Mortgage \$748,000 for repeatedly violating the National Do-Not-Call rules. The FCC's Order imposed the maximum forfeiture of \$11,000 on each of the 68 calls made by Dynasty to a total of 50 consumers that violated National Do-Not-Call laws. Notably, the FCC's Order found that Dynasty could not take shelter under the safe harbor for National Do-Not-Call violations because it did not properly seek access to the National Do-Not-Call database and failed to implement routine procedures, including the adequate training of personnel, to comply with the National Do-Not-Call rules.

A copy of the FCC's Order can be found at:
http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-67A1.doc.

VI. CONSUMER PROTECTION

- **New York Files Suit Against Dell** – New York Attorney General Andrew M. Cuomo announced on May 16 that his office had filed suit against Dell and its financial services unit, alleging that they engaged in several deceptive business practices. The Attorney General said the suit was filed after an investigation and receipt of more than 700 complaints by Dell customers in the state of New York. Dell responded that this number represents a very small fraction of its transactions in New York. The lawsuit was filed in Albany County Supreme Court and alleges that Dell used bait-and-switch tactics with its financing options—its promotional offers claimed that financing was interest-free when in fact many customers faced interest rates as high as 29%. The lawsuit alleges additional deceptive business practices related to Dell's technical support services, rebate offers, and billing and collections activity.



The lawsuit seeks restitution, civil penalties, and the adoption of measures that prevent the alleged deceptive practices in the future. In light of this lawsuit, companies would do well to evaluate their consumer-facing practices including customer service and billing and collections to ensure that they are in compliance with both federal and state laws in this area.

VII. INTERNATIONAL AFFAIRS

U.K. – Information Commissioner's Office Approves Philips' Binding Corporate Rules – On May 9, the United Kingdom's data protection office, the Information Commissioner's Office (ICO), issued its second approval of a company's binding corporate rules. Pursuant to this authorization, Philips is permitted to share the personal data of its employees and clients on a company-wide basis and to transfer the data outside the EEA because the ICO was assured that Philips had "the necessary procedures in place" to safeguard the information and that there was "an adequate level of protection for individuals' rights and freedoms" across the Philips' group of companies. It should be noted, however, that this authorization only applies to information that falls under the Information Commissioner's jurisdiction, specifically, information that is held in the UK.

The UK Information Commissioner's official announcement is available at
http://www.ico.gov.uk/upload/documents/pressreleases/2007/philips_authorized_by_ico_to_transfer_personal_information.pdf.

VIII. STATES

- **Children's Protection Registry Act in Utah Under Scrutiny** – Two years after passage, and 18 months of litigation, the Children's Protection Registry Act in Utah is under scrutiny for costing Utah residents a significant amount of money. As reported in previous *Privacy and Data Security Briefings*, the Registry, which charges companies every time they access the database to compare the Registry with their email database, was touted as a money-making venture by legislators and the initial author of the bill, Matthew Prince of Unspam. Unspam is the vendor for the Registry, and is designed to receive a portion of each transaction. The volume of companies accessing the Registry has been minimal, as companies either suppress Utah-based email addresses, attempt to not send "high risk" commercial email, or take a risk on enforcement. The Registry law has been challenged in federal District Court, and the state of Utah has paid Brent Hatch, son of U.S. Senator Orrin Hatch, over \$100,000 to defend the lawsuit on Unspam's and the state's behalf so far. The *Salt Lake Tribune* has been covering these issues in some detail; its initial article on the Hatch representation, plus Prince's rebuttal, are attached below.

The *Salt Lake Tribune's* initial expose is available at:
http://www.sltrib.com/search/ci_5778185

Unspam CEO Prince's rebuttal available in the *Salt Lake Tribune* at:
http://www.sltrib.com/search/ci_5882321.



May 22, 2007 – June 4, 2007.

I. PRIVACY

- **Congressman Questions Plan to Collect Data from Online Sellers** – On May 22, 2007, Representative Tom Davis (R-VA) sent a letter to U.S. Treasury Secretary Paulson, questioning an administration proposal that would require websites such as eBay and Amazon.com to file income statements with the IRS for all customers who use their sites to conduct 100 or more separate transactions that generate \$5,000 or more per year. Such websites would be required to collect customers' names, addresses, and taxpayer identification numbers or Social Security numbers. This proposal was discussed in the previous issue of the *Privacy and Security Briefing*. Representative Davis noted his concern about the privacy and security of taxpayer information if such a proposal moves forward. He requested that a Treasury Department official brief his committee staff on plans for safeguarding the data.

A press release and copy of Representative Davis's letter are available at: <http://republicans.oversight.house.gov/News/PRArticle.aspx?NewsID=179>.

- **Direct Marketing Association Provides Guidance Regarding Use of Marketing Lists** – The Direct Marketing Association (DMA) recently reminded its members to follow its guidance regarding the sharing of marketing lists. While list providers may believe they are not responsible for the actions of marketers with whom they share their customers' data, list providers may be held responsible for consciously avoiding knowledge about a legal violation involving the use of the data. Accordingly, those who sell or share marketing lists are advised by the DMA to obtain a copy of the script or email that will be used to market to the list; monitor list usage to ensure that it is only used for appropriate purposes; and have a written agreement stating the purpose and scope of the list's usage.

An article on this issue is available at: <http://www.dmnews.com/cms/dm-news/shows-assns/41230.html>.

II. SECURITY

- **Credit Protection Costs Do Not Support a Data Breach Negligence Claim** – A U.S. District Court in Ohio has held that the cost of credit monitoring is not sufficient damage to support a claim of negligence following a data breach (*Kahle v. Litton*, S.D. Ohio, No 1:05cv756). The suit stems from a break-in at Litton Loan Servicing that included the theft of hard-drives containing the personal information of nearly 230,000 former customers of Provident Bank, include Patricia Kahle. Litton said the hard-drives were password protected and needed to be arranged in certain order to function properly. Kahle enrolled in a credit protection service costing \$2.99 a month. In the 20 months since the theft of the data, there was no indication Kahle's information was inappropriately accessed. The court concluded that "[w]ithout direct evidence that the information was accessed or specific evidence of identity fraud this Court can not find the cost of obtaining ... credit monitoring to amount to damages in a negligence claim."



This decision follows the basic reasoning of *Key v. DSW* and *Guin v. Brazos Higher Educ. Serv. Corp.* In both cases, district courts found that the possibility of identity theft was speculative and therefore insufficient to support a claim.

A copy of the *Kahle* decision is available at: <http://pub.bna.com/eclr/05cv00756.pdf>.

- **Minnesota Enacts Law Making Merchants Responsible for Data Breaches** – Minnesota Governor Tim Pawlenty (R) has signed H.F. 1758, the first law in the country that makes merchants who retain credit and debit card information for too long liable to banks if that data is then lost or stolen. The law would require merchants to destroy magnetic stripe data from credit cards immediately after processing the transaction. Debit card magnetic stripe data could be retained for 48 hours following the transaction. If merchants do not follow these requirements and the data is lost or stolen, banks can then seek to recoup costs for:
 - canceling and reissuing credit cards
 - closing and/or reopening accounts affected by the breach
 - stop payment actions
 - unauthorized transaction reimbursements
 - providing of breach notice to affected individuals

Similar legislation is being considered in California, Connecticut, Illinois, and Massachusetts. The Texas legislature considered such a bill, which also included a requirement that retailers to follow the Payment Card Industry Data Security Standards. These detailed standards are promulgated by the major credit card associations and companies. The Texas legislature has since adjourned and that bill will need to be reintroduced next session. Even absent such statutory authorization, banks have tried to recoup the costs of reissuing cards following a breach. TJX, for example, is facing a class action suit from banks who had to reissue cards following the theft of over 45 million cards numbers from the retailer.

This issue has also arisen in the debate over the need for federal data security legislation. Congressman Barney Frank (D-MA), the Chairman of the House Financial Services Committee, has said that data breach legislation being considered by his committee will hold retailers responsible if they cause the breach.

A copy of the bill is available at: <http://www.revisor.leg.state.mn.us/bin/getbill.php?session=ls85&number=HF1758&version=list>.

- **Federal Legislative Update** – The Senate Judiciary Committee has reported out two data security bills to the full Senate.



- o S.495, introduced by Senators Patrick Leahy (D-VT) and Arlen Specter (R.PA) the chairman and ranking member of the Committee, which would establish breach notification standards and basic data safeguards and create additional requirements for data brokers. *See* the February 21, 2007 *Privacy and Data Security Briefing* for an overview and analysis of S.495.
- o S.239, introduced by Senator Dianne Feinstein, which contains the same data breach notification requirements as S.495, without the data safeguard or data broker requirements.

As reported in previous *Privacy and Data Security Updates*, S.495 will need to be reconciled with a bill being considered in the Commerce, Science and Transportation Committee.

III. SPYWARE

- **House Scheduled to vote on SPY Act** – As reported in the most recent *Privacy and Data Security Briefing*, an anti-spyware bill that would require notice and consent before personally identifiable information about a user is collected by a Website was approved by the House Energy and Commerce Committee on May 10, 2007. The House is scheduled to vote on HR 964 today, June 6.

Text of the legislation as it passed Energy and Commerce is available at: http://energycommerce.house.gov/cmte_mtg/110-fcmu.051007.hr964.hr948.shtml.

- **Zango Sues PC Tools Over Spyware Classification** – Downloadable software distributor Zango, formerly 180solutions, has filed a suit against Spyware Doctor software maker PC Tools, seeking over \$35 million in damages and an injunction. The suit alleges that PC Tools misclassifies and removes Zango software from users' computers without warning or consent thereby libeling Zango, tortiously interfering with its contractual rights, and violating Washington State's Consumer Protection Act. The current Spyware Doctor Starter Edition rates Zango's software as an "elevated threat." PC Tools replied in a statement that it believed Zango's suit was "an attempt by Zango to influence [its] reclassification process." Private anti-spyware companies have been applying differing standards of "threat" designation, often with some element of fear and quantity of software applications incorporated in order to increase purchases of the anti-spyware software. Zango is utilizing tort and contract claims to attempt to ameliorate this circumstance.

The full text of the IDG News Service article is available at: http://www.infoworld.com/article/07/05/18/zango-sues-antispysware-vendor_1.html.

Zango's complaint is available at: <http://blogs.csoonline.com/files/complaint.pdf>.



IV. SPAM

- **FTC Focuses on Spam** – The widely reported rise in spam is receiving renewed attention from the Federal Trade Commission. During a recent Direct Marketing Association event, Eileen Harrington, the FTC deputy director of consumer protection, stated that the FTC is particularly concerned about the claimed rise in malicious spam, including "phishing" messages. Harrington highlighted recent reports that indicate only about 25 percent of Fortune 500 companies are authenticating their e-mail. She also stated that the FTC wants Internet service providers to take steps to apply "negative scoring" to unauthenticated e-mail.

As reported in previous issues of the *Privacy and Data Security Briefing*, the FTC has already announced a spam summit that will be held in July during which they will specifically examine strategies to protect consumers and businesses from malware and phishing attacks. Harrington noted that the summit is not necessarily aimed at launching a request for new legislation because CAN-SPAM has generally been effective in combating spam.

An article about this speech is available at: <http://pubs.bna.com/NWSSTND/IP/BNA/eip.nsf/SearchAllView/00329E2010EAC547852572E20072C4ED?Open&highlight=HARRINGTON>.

- **Infamous Spammer Prosecuted** – One of the reported "world's biggest spammers," Robert Soloway, was arrested in Seattle for allegedly using zombies or botnets (secretly infected computers) to send out millions of e-mails. Interestingly this spam was aimed at selling tools and services to companies that would allow them to send their own junk e-mail.

Prosecutors allege that Soloway has sent millions of junk e-mails since 2003, even after Microsoft Corp. successfully obtained a \$7 million civil judgment against him in 2005 and another smaller Internet service provider won a \$10 million judgment.

Reports describe Soloway as one of, if not the, world's biggest spammer and he appears on a Spamhaus list of the spammers deemed responsible for as much as 80 percent of all junk e-mail. Nonetheless, commentators remarking on the arrest stated that shutting down Soloway will have little real effect on the rise in spam. This may be especially true as other spammers, many of whom are reportedly based in Russia and other countries beyond the reach of U.S. or European law, have surpassed Soloway.

Soloway was indicted on charges of mail fraud, identity theft, and money laundering and if convicted, could face a fine of \$250,000 and a prison term of up to 65 years.

An article about this development is available at: http://news.yahoo.com/s/ap/20070531/ap_on_hi_te/spam_arrest.



- **Public Access to Central Database With Phishing Attacks Announced** – The Anti-Phishing Working Group has announced that beginning in July it will share information about phishing attacks and trends that will be stored in a central database. The purpose of the database will be to increase tracking and destruction of phishing attacks.

An article about this development is available at:

<http://scmagazine.com/uk/news/article/659251/anti-phishing-database-laun>.

- **E-mail Authentication Framework Established** – The Internet Engineering Task Force, a group responsible for technical standards on the Internet, has approved e-mail authentication framework DomainKeys Identified Mail (DKIM) as proposed standard RFC 4871. DKIM gives message authentication, verification, and traceability to help determine whether a message is legitimate. It also provides information to Internet service providers and consumers to assist them in confirming the true identity of a message's point of origin. This is the most recent attempt to create an email authentication methodology; it is unclear how successful this effort will be.

An article about this development is available: <http://www.dmnews.com/cms/dm-news/e-mail-marketing/41233.html>.

- **Pirates of the Caribbean Spam Includes Malware** – A Pirates of Caribbean related e-mail promising a trailer for *Pirates of the Caribbean 3: At World's End* and the chance to obtain free tickets in fact downloads a Trojan Horse on unsuspecting consumers. Once the malware is downloaded onto a consumers computer, hackers can obtain consumers' information for identity theft and other crimes. This is just the latest scam in which hackers rely on well-known brands to reach unsuspecting consumers. This attack is related to the issues addressed by FTC's Eileen Harrington, referenced above.

An article about this development is available at:

<http://www.securecomputing.net.au/news/52927/pirates-of-the-caribbean-spam-spreading.aspx>.

V. TELECOM/WIRELESS

- **FCC Seeks Comment on DoJ Petition Seeking Modification of the CALEA Standard So More Data Can Be Gathered From Wireless Telephone Taps** – On May 25, 2007, the FCC placed on Public Notice a Petition for Expedited Rulemaking filed by the Department of Justice seeking a modification of the technical standard commonly used under CALEA so that law enforcement agencies can gather data transmissions sent by wireless telephones. The modifications sought by the DoJ would include packet activity reporting, time-stamp information, all reasonably available handset location information, and other carrier security, performance and reliability requirements. The DoJ claims that without this additional information, important public safety and national security objectives would be at risk. Comments are due by June 25, 2007, and reply comments are due by July 25, 2007.



Copies of the DoJ's Petition and the FCC's Public Notice can be found at:

http://gulfoss2.fcc.gov/cgi-bin/websql/prod/ecfs/comsrch_v2.hts. If you experience trouble accessing the documents through this link, please contact us and we will provide you with a copy.

- **Nebraska Governor Vetoes Legislation to Limit Automated Political Calls** – On May 21, 2007, Nebraska Governor David Heineman (R) vetoed LB-198, a bill to limit the transmission of autodialed prerecorded political telephone calls to consumers in the state. The bill would have limited political parties to two such calls per day and would have prohibited such calls entirely before 8 a.m. and after 9 p.m. Notably, Governor Heineman indicated that his principal objection to the bill was that it proposed to restrict only political speech – not all autodialed prerecorded calls – and therefore was vulnerable to Constitutional attack. Governor Heineman suggested that he would be open to considering a broader bill, and one is expected to be introduced in the next legislative session.

Additional information about LB-198 and the Constitutional analysis on which Governor Heineman relied can be found at:

http://uniweb.legislature.ne.gov/Apps/BillFinder/finder.php?page=view_doc&DocumentID=567.

- **Senate Intelligence Committee Rejects (For Now) Phone Company Immunity in Connection with NSA Warrantless Surveillance Program** – The Senate Intelligence Committee has rejected – for the time being – a proposal by the Bush Administration to protect telephone companies from liability in connection with their participation in the NSA's warrantless surveillance program. The Committee made its announcement in a report released on May 31, 2007, in connection with Senate bill 1538, the Fiscal Year 2008 Intelligence Authorization Act. According to the Committee, its decision was based largely on the Administration's refusal to comply with certain document requests intended to enable the Committee to better evaluate the proposal, and, more generally, a number of other provisions in the Act. The immunity proposed in S.1538 would apply retroactively to September 11, 2001, as well to future surveillance activities. Both the Senate and House Intelligence Committees approved legislation earlier this year to update the Foreign Intelligence Surveillance Act, but that legislation did not include telephone company immunity for participation in warrantless surveillance.

Additional information about S.1538 can be found at: <http://thomas.loc.gov/cgi-bin/bdquery/D?d110:1:./temp/~bdl04:@@L&summ2=m&/bss/110search.html#major%20actions>:

- **Verizon Wireless Sues Wireless Text Spammer** – On June 1, 2007, Verizon Wireless filed a lawsuit against I-Vest Global Corp., alleging that I-Vest illegally attempted to transmit more than 12 million text messages promoting stock and real estate schemes to Verizon Wireless subscribers. Such transmissions are prohibited under the FCC's rules absent subscriber consent and also are barred by certain state telemarketing and privacy laws. Verizon Wireless claims that, to date, only 5,000 of I-Vest's text messages were



delivered because of robust spam filtering software Verizon Wireless has installed on its network. Verizon is seeking a preliminary injunction against I-Vest as well as monetary damages.

Additional information about the Verizon Wireless lawsuit can be found at: <http://www.njbiz.com/article.asp?aID=70918>.

VI. STATES

- **ChoicePoint Reaches Additional Settlement with 44 Attorneys General Relating to Its Privacy Practices in 2005** – On May 31, 2007, ChoicePoint announced that it had reached a settlement with 44 Attorneys General relating to its privacy and data security practices in 2005. As reported in numerous *Privacy and Data Security Briefings*, in February 2005, ChoicePoint announced that criminals posing as legitimate businesses gained access to consumers' personally identifiable information. In the wake of these crimes, ChoicePoint, notified more than 145,000 consumers whose information may have been viewed or acquired by the criminals. This episode has triggered many of the over three dozen state data breach notification laws.

ChoicePoint had previously settled with the Federal Trade Commission for \$5 million in consumer redress and \$10 million in fines. This settlement purports to go beyond the FTC settlement and requires ChoicePoint to improve its credentialing process for clients that obtain Social Security numbers and other forms of personally sensitive information. The Attorneys General of the following states participated in the settlement: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Hawaii, Idaho, Illinois, Indiana, Iowa, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Tennessee, Texas, Vermont, Virginia, Washington, West Virginia, Wisconsin and the District of Columbia. Also as part of this settlement, ChoicePoint will pay \$500,000 to the states.

The settlement itself does not appear to be available publicly.

VII. RADIO FREQUENCY IDENTIFICATION TECHNOLOGIES (RFID)

- **California State Senate Passes the Identity Theft Information Protection Act of 2007 (SB 30)** – The California State Senate has passed one of the five RFID bills that we reported on in the April 16 *Privacy and Data Security Briefing*. Specifically, on May 24, 2007, the State Senate passed the broadly-supported Identity Information Protection Act of 2007 (SB 30), which creates privacy and security safeguards for existing RFID-enabled government IDs. In particular, the bill would, among other things:
 - Require certain identification documents (as defined) that are created, mandated, purchased, or issued by a state, county or municipal government that use radio waves to transmit data, or to enable data to be read remotely, to



meet specified requirements, including, among other things, incorporating tamper-resistant features, implementing an authentication process, and using mutual authentication, encryption methods, and access control protocols where personally identifiable information is transmitted remotely.

- Exempt certain types of contactless identification document systems, including certain systems existing as of January 1, 2008, and identification documents issued to incarcerated or detained individuals, to law enforcement officers and emergency response personnel as well as to certain types of patients under the care of a government-operated or -owned facility.
- Authorize declaratory or injunctive relief or a writ of mandate and attorney's fees and costs under certain circumstances.
- Require the California Bureau of Research to submit a report to the Legislature on security and privacy for government-issued, remotely readable identification documents. In order to prepare the report, the Bureau would need to establish an advisory board, to be comprised of specified government officials and representatives from industry and privacy rights organizations, to make recommendations and provide technical advice to the Bureau.

The provisions of the legislation would sunset as of December 31, 2013. The bill has been sent to the State Assembly for consideration. A similar version of the bill passed both houses last year, but was vetoed by Governor Schwarzenegger. The Governor has not yet stated his position on the bill, but the bill reportedly has broad nonpartisan support.

Text of the legislation can be found at: http://www.leginfo.ca.gov/pub/07-08/bill/sen/sb_0001-0050/sb_30_bill_20070419_amended_sen_v97.html.

An article addressing the new legislation can be found at: <http://arstechnica.com/news/ars/post/20070525-rfid-security-act-passed-by-california-senate-again.html>.

A non-related article generally discussing the growing backlash against RFID can be found at: <http://money.cnn.com/2007/05/21/technology/rfid/>.

- **Privacy and Security Concerns Voiced at 2007 Canadian RFID Conference** – At the 2007 Canadian RFID Conference in Markham, Ontario, Melanie Millar-Chapman, Office of Privacy Commissioner of Canada, urged developers and suppliers of RFID technologies to build privacy into their products now before the law requires it. Millar-Chapman noted that there are both privacy and security concerns with RFID. On the privacy side, there is a risk of privacy invasion with RFID to the extent that the information collected through tags can be linked to personal information. On the security side, there is a risk of identity theft, intercepted communications, and infestation of tags with malicious codes. She also cautioned RFID developers to consider implications of RFID in the workplace where many employers already collect data to keep track of



employees. Industry representatives at the conference acknowledged the privacy and security concerns, but noted that building privacy and security into RFID is driving up the cost of the technologies and widespread implementation of RFID depends on bringing prices down.

An article discussing the 2007 Canadian RFID Conference can be found at:
http://www.sptnews.ca/index.php?option=com_content&task=view&id=648&Itemid=9.

June 5, 2007 – June 20, 2007.

I. PRIVACY

- **Sixth Circuit Decides Email Privacy Case** – The Sixth Circuit Court of Appeals ruled on June 18, 2007, that federal investigators overstepped constitutional and statutory bounds by searching emails without obtaining a warrant during an investigation involving an herbal supplement company called Berkeley Premium Nutraceuticals. The unanimous decision by the three-judge panel upholds a lower-court ruling that temporarily blocked investigators from conducting additional email searches in the case against the company's owner, Steven Warshak. Warshak, who pleaded not guilty to charges that he defrauded customers and banks out of at least \$100 million, argued that his Fourth Amendment right not to be subject to unreasonable searches and seizures was violated by investigators.

The court held that "individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP." Citing *Katz v. U.S.*, the seminal Fourth Amendment case holding that individuals have an expectation of privacy regarding telephone calls, the court held that a similar expectation existed regarding email. As such, the court prohibited the government from "seizing the contents of a personal e-mail account maintained by an ISP in the name of any resident of the Southern District of Ohio, pursuant to a court order issued under 18 U.S.C. § 2703(d) [part of the Stored Communications Act of the Electronic Communications Privacy Act], without either (1) providing the relevant account holder or subscriber prior notice and an opportunity to be heard, or (2) making a fact-specific showing that the account holder maintained no expectation of privacy with respect to the ISP, in which case only the ISP need be provided prior notice and an opportunity to be heard."

Commentators have stated that the ruling has major implications for Internet privacy. It remains to be seen how this decision will affect other pending cases and investigations, and whether it will be appealed to the full Sixth Circuit or to the Supreme Court.

The decision in *Warshak v. U.S.* is available at:
<http://www.ca6.uscourts.gov/opinions.pdf/07a0225p-06.pdf>.



An article on this issue is available at:
<http://www.chron.com/dispatch/story.mpl/ap/fn/4899746.html>.

- **Google's Privacy Practices Continue to Make News** – Google announced that it would limit the amount of time that it retains personally identifiable data obtained from its users to 18 months. In March, Google had stated it would retain such information for 18-24 months. The EU Justice and Security Commissioner commended Google's decision. The EU group is currently looking into Google's privacy practices but has stated that it will not make a final decision before October on whether Google may be violating European privacy laws.

Google's new map service, Street View, is currently available in select U.S. cities and offers street-level images of particular addresses. The service has raised privacy concerns due to the clarity and detail of the images, which have caused some to view it as an invasion of personal privacy. Google has stated that the service shows "what any person can readily capture or see walking down the street" and thus in the public domain, without a reasonable expectation of privacy. Nonetheless, the publication and memorialization of these events has some people unnerved, even if the photos are of public spaces. Google allows users to request the removal of an image for privacy reasons.

In a report released June 9, London-based Privacy International assigned its lowest privacy grade – a rating used for companies with "comprehensive consumer surveillance and entrenched hostility to privacy" – to Google. Google responded that it stands by its privacy practices and was disappointed with the rating and accompanying report, which it said were based on inaccuracies and misunderstandings about Google's services.

Google's EU Privacy Counsel, Peter Fleischer, stated in an interview that Google is considering visibility that would allow users to view the personal information the company has collected about them.

An article on Google's new data retention period is available at:
<http://www.washingtonpost.com/wp-dyn/content/article/2007/06/13/AR2007061300727.html>.

An article on Google's Street View is available at:
<http://www.rtoonline.com/Content/Article/may07/GoogleEarthStreetLevelView053107.asp>.

An article on Google's privacy rating is available at:
<http://www.washingtonpost.com/wp-dyn/content/article/2007/06/09/AR2007060900840.html>.

An article on the interview with Peter Fleischer is available at:
<http://news.zdnet.co.uk/software/0,100000121,39287507,00.htm>.



- **Study Finds Online Shoppers Will Pay More for Increased Privacy Protection** – A study conducted by Carnegie Mellon University found that on average, consumers were willing to pay about sixty cents extra on a fifteen dollar purchase when they were satisfied with the website's privacy policy. The study provided consumers with information about websites' privacy practices and gave them a financial incentive (they were able to keep any excess money) to make their purchases from less expensive sites. The majority of people chose to purchase from websites with high privacy ratings. The researchers posited that consumers want to protect their privacy but don't always know where to obtain or how to interpret information a website posts about its own privacy practices.

An article on this issue is available at:
<http://www.networkworld.com/news/2007/060607-privacy-confidence-survey.html>.

- **Direct Marketing Association (DMA) Issues Revised Guidelines for Data Compilers** – The DMA has issued revised guidelines for data compilers, which it defines as “any company that assembles personally identifiable information about consumers (with whom the compiler has no direct relationship) for the purpose of facilitating the renting, selling, or exchanging of information to non-affiliated third-party organizations for marketing purposes.” The revised guidelines are intended to strengthen and clarify provisions within the DMA's Guidelines for Ethical Business Practice that relate to the collection and sharing of consumer information by data compilers

An article on this issue is available at: <http://www.dmnews.com/cms/dm-news/database-marketing/41455.html>.

The guidelines are available at: <http://www.the-dma.org/guidelines/DatabaseCompilers/>.

II. SECURITY

- **Debate over paying for breach remediation escalates** – As noted in the June 6, 2007 *Privacy and Data Security Briefing*, financial institutions and merchants are debating who should be responsible for paying the costs associated with, particularly the costs of reissuing compromised debit and credit cards. These costs are typically covered by the financial institutions, who argue that if retailer's lax data security practices are responsible for the breach, the retailer should pay to reissue the cards. Banks and credit unions have filed several law suits to recoup such costs following a breach.

As noted in prior *Briefings*, Minnesota has enacted a law allowing financial institutions to recoup these costs and House Financial Services Committee Chairman Barney Frank (D-MA) has suggested he would include similar provisions in data security legislation the committee is considering. This debate has continued to evolve, with the following notable developments:

- The House Small Business Subcommittee on Finance and Tax held a hearing on the impact of data security bills on June 6. Included in the testimony were



disparate views on whether Congress should allocate the costs of data breaches. John Milazzo, the chairman of the National Association of Federal Credit Unions, told the subcommittee that Congress should follow the Minnesota model to ensure retailers paid these costs when appropriate. Mallory Duncan, senior vice president and general counsel of the National Retail Federation disagreed and urged the subcommittee to leave the allocation of costs to private sector mechanisms like the Payment Card Industry Data Security Standards (PCI DSS).

Testimony from the House Small Business Committee hearing is available at: <http://www.house.gov/smbiz/hearings/hearing-06-06-07-sub-data/hearing-06-06-07-sub-data.htm>.

- California reversed course and removed a provision in A.B. 779 that would have allowed banks to seek reimbursement from a merchant for the costs of sending notices and reissuing cards. Following that amendment, the bill passed the Assembly 58-2. A.B. 779 is now being considered in the State Senate.

A copy of A.B. 779 is available at: http://info.sen.ca.gov/pub/07-08/bill/asm/ab_0751-0800/ab_779_bill_20070601_amended_asm_v95.pdf

III. SPYWARE

- **House Passes Amended Spy Act Over Industry Objections** – In what has become a biannual tradition, the U.S. House of Representatives passed the *Securely Protect Yourself Against Cyber Trespass Act* or *SPY ACT*, albeit with a modicum of opposition this time, by a vote of 368-48. The legislation, H.R. 964, sponsored by Ed Towns (D-NY) and Mary Bono (R-CA), aims to combat the practice of surreptitiously downloading information gathering programs onto unsuspecting users by requiring websites to give notice to and receive consent from users before engaging in those practices.

The legislation also includes a “good Samaritan” provision for software providers who, in good faith, provide software to users that remove or disable spyware prohibited by the Act.

The legislation has attracted significant opposition by the business community however. Critics, such as the U.S. Chamber of Commerce, argue that as passed, Section 3 of the Act goes far beyond regulating spyware and affects every legitimate website that collects information from its users including subscribers to newsletters and users requesting more information from the website. The Chamber was one of 31 signatories of a June 5 letter to lawmakers objecting to the bill.

Supporters of the Act defended the legislation noting that the Act allows the Federal Trade Commission to modify or exempt websites from the notice and consent requirements of the Act where users have adequate notice regarding the uses of information that is inputted directly into a field on that website. A version of the



legislation has passed the House in the previous two Congresses but died both times in the Senate.

The full text of H.R. 964 as reported to the Senate is available at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h964rfs.txt.pdf

A letter from the U.S. Chamber of Commerce to members of the U.S. House of Representatives in opposition to H.R. 964 is available at: <http://www.uschamber.com/issues/letters/2007/070605cyber.htm>.

- **FTC Warns Company Executives About Bogus Email Claiming to be from the Agency** – On June 18, 2007, the FTC issued a press release warning consumers, including corporate executives, about a bogus email that appears to be from the FTC acknowledging receipt of a complaint. The email is actually from third parties attempting to download spyware onto recipients' computers. The e-mail is personalized, containing the name of the recipient and their business. The message explains how the complaint will be used, who will have access to it, and states, "Attached you will find a copy of your complaint. Please print a hard copy of the complaint for your records in the upcoming investigation." This attachment, if opened, will install malicious spyware onto the recipient's computer. The FTC has warned recipients of this email not to open the attachment, to delete the email, and to empty the deleted items folder. We are aware of several instances of executives receiving this email, and we emphasize that the attachment should not be opened.

The FTC's press release is available at: <http://ftc.gov/opa/2007/06/email.shtm>.

IV. SPAM

- **More Service Providers Sign-up for Email Certification Program** – Comcast, Cox Communications, Time Warner Cable's Road Runner, and Verizon are joining Goodmail System Inc.'s email certification program. Goodmail allows certified bulk emailers to bypass anti-spam filters upon paying a ¼ cent per message fee. As reported in earlier editions of the *Privacy and Data Security Briefing*, AOL and Yahoo already joined the Goodmail program amid much controversy. With the addition of the other service providers, Goodmail reports that its program now includes approximately 65 percent of consumer email users in North America. Goodmail also reports that approximately 400 brands, 150 governmental agencies, and a dozen non-profits have are sending Goodmail certified email.

Goodmail is yet another method whereby marketers are seeking to respond to the fight against spam so that they may reach consumers through email. Goodmail can be expected to expand its presence online as anti-spam filters become more robust.



An article about this development is available at:

http://home.businesswire.com/portal/site/topix/index.jsp?ndmViewId=news_view&newsId=20070607005249&newsLang=en&ndmConfigId=1000639&vnsId=41

- **Email Harvesting Case Can Proceed** – A California court has ruled that a competitor's email harvesting activities could violate California's penal code and be actionable as misappropriation. See *Facebook Inc. v. ConnectU LLC, N.D. Cal., No. 07-01389, 5/21/07*. Plaintiff and social networking site, Facebook Inc., filed a lawsuit against its competitor, ConnectU LLC, after ConnectU obtained hundreds of Facebook users' email addresses, and subsequently began sending them messages to get them to switch to ConnectU. ConnectU filed a motion to dismiss, which the court denied in part. The court allowed Facebook's arguments under the California Penal Code and its common law misappropriation claim to proceed, but dismissed its claims brought under California's spam statute and CAN-SPAM as inapplicable as pled.

Notably, the California court held that ConnectU's email harvest did fall within California's Penal Code provision section 502(c) which makes it a "public offense" when a person to "knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network." The court rejected ConnectU's argument that the email addresses were voluntarily supplied by users who authorized their use, and, instead, maintained that Facebook authorization was required. The court also held that the claims were not preempted by the federal Copyright Act.

A copy of the court's opinion is available at:

http://pub.bna.com/eclr/07cv1389_052107.pdf

An article about this development is available at:

<http://pubs.bna.com/NWSSTND/IP/BNA/eip.nsf/SearchAllView/3F568CD45633117B852572F1007C66F7?Open&highlight=CONNECTU>

- **FBI Announces Campaign to Fight Online Fraud** – The FBI has announced "Operation Bot Roast," a campaign to fight online computer zombies. Computer zombies secretly gain access to users' computers and direct the computers to a specific website. After creating network of computers all directed to one website, the hacker can overwhelm their servers and possibly shut them down. The zombies can also be used to spread spam or steal user IDs.

Under the FBI campaign, the FBI will contact users whose computers have been hijacked through these scams. To date, the FBI has already notified one million PC owners who it knows to be part of a zombie network. The FBI has also made three arrests of alleged perpetrators of zombie networks.

An article about this development is available at: http://news.com.com/8301-10784_3-9729203-7.html



V. TELECOM/WIRELESS

- **House Passes Second Anti-Spoofing Measure to Address Caller ID Misuse; Senate Commerce Committee Also to Consider Issue** – On June 11, 2007, the House Energy and Commerce Committee approved an amended version of H.R. 251, the “Truth in Caller ID Act,” which is intended to prohibit the manipulation of Caller ID information. As a general matter, the bill would make it unlawful for any person within the U.S. to cause any telecommunications- or VoIP-related caller identification service to transmit misleading or inaccurate Caller ID information with the intent to defraud or cause harm. The bill would not, however, prevent or restrict the use of Caller ID blocking. The bill would require the FCC to prescribe regulations implementing its provisions within six months of the bill’s passage. In doing so, the FCC would have to consider requiring all non-commercial calls transmitted via autodialer or prerecorded voice to include Caller ID information. The FCC’s current rules require all telemarketing calls except those transmitted by tax-exempt organizations to include Caller ID information.

The Senate Commerce Committee, for its part, has announced that it will hold a hearing on June 21, 2007, to consider S.704, the Senate version of the “Truth in Caller ID Act,” which was introduced by Senator Bill Nelson (D-FL) on February 28, 2007.

Earlier this year (on March 21, 2007), the House Judiciary Committee passed H.R. 740, the Preventing Harassment through Outbound Number Enforcement (PHONE) Act, which also would make it unlawful to transmit false Caller ID information with the intent to defraud or deceive. The principal difference between H.R. 251 and H.R. 740 is that while the former would rely on existing enforcement provisions in the Communications Act (fines of up to \$10,000 and/or up to a year in prison), H.R. 740 includes more stringent enforcement mechanisms, such as fines, forfeitures, and/or up to five years in prison.

Copies of H.R. 251, S.704 and H.R. 740 can be found at: <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.00251>; <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:s.00704>; and <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.00740>.

- **Additional Bill Authorizing Further Funding National Do-Not-Call Registry Introduced in House** – On June 6, 2007, Representative Cliff Stearns (R-FL) introduced H.R. 2601, which would authorize funding of the Do-Not-Call Implementation Act – and, thus, the National Do-Not-Call registry – for an additional five years, through 2012. In the Senate, a similar bill (S.781) was introduced by Senator Mark Pryor (D-AR) on March 6, 2007, although that bill would fund the Do-Not-Call Implementation Act indefinitely. Neither bill has advanced thus far in either body.

Copies of H.R. 2601 and S.781 can be found at: <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.02601>; and <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:s.00781>.



June 18, 2007 – July 9, 2007.

I. PRIVACY

- **Yahoo Launches Personalized Advertising System** – On July 2, Yahoo launched SmartAds, an advertising system that will let marketers tailor advertising content to individual users. The system uses behavioral, demographic, and geographic information about users in order to deliver more personalized ads. Privacy advocates, such as the Center for Democracy and Technology, raised concerns as to how long Yahoo will store the data it collects about users and whether users will have any control over the data. Behavioral targeting and tailored advertising, as indicated by the recent acquisition bids in this area by Yahoo, Microsoft, and Google, continues to be seen as a growth area.

An article on this issue is available at: <http://www.washingtonpost.com/wp-dyn/content/article/2007/07/02/AR2007070201744.html>.

II. SECURITY

- **GAO Report Finds Little Link Between Breaches and ID Theft** – Responding to a Congressional request to study the issue, the Government Accountability Office (GAO) concluded that the overwhelming majority of data breaches do not result in account fraud or identity theft. Of the 24 largest data breaches reported between 2000 and 2005, the report found that only four resulted in fraud. The request for the report was led by the ranking member on the House Financial Services Committee, Congressman Spencer Bachus (R-AL), and could be used as evidence to support the need for a strong risk-based trigger in the breach notification bill the Committee is planning on considering.

A copy of the GAO Report is available at: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-737>

III. SPYWARE

- **FTC Commissioner Leibowitz Dissents from Commission’s Settlement with DirectRevenue** – The FTC Commission approved a final settlement with DirectRevenue, LLC. In a dissenting statement issued on June 26, FTC Commissioner Jon Leibowitz praised the Commission’s imposition of “strong injunctive relief” in the FTC’s final settlement, but registered his “disappointment” with the \$1.5 million in monetary relief imposed under the settlement because it “leaves DirectRevenue’s owners lining their pockets with more than \$20 million from a business model based on deceit.” As reported in previous *Privacy and Data Security Briefings*, according to the FTC complaint, DirectRevenue downloaded “nuisance” adware, which delivered pop-up advertising to consumers, without notice and consent, and sometimes bundled its adware with software that purported to block such pop-up advertisements. Leibowitz decried this activity as “the height of cynicism and disingenuousness.” He added that while he understood that settlements involve “compromise, and staff must weigh the advantages of a settlement



with risks and costs of litigation," he would prefer litigation in such a case and "risk losing [rather] than settl[ing] for a compromise that makes an FTC action just a cost of doing business."

Links to the Complaint, Decision and Order, news release, and Commissioner Leibowitz's dissent are available at: <http://www.ftc.gov/os/caselist/0523131/index.shtm>.

- **Bold Spyware Scam Spoofs FTC** – As mentioned in the most recent *Privacy and Data Security Briefing*, on June 18, the FTC released an advisory in which they warned consumers that third parties sent fraudulent emails to consumers in which the third parties represent themselves as the FTC. The emails purport to be the FTC's acknowledgement of the consumer's (or company's) complaint to the agency and contain an attachment purporting to be a copy of the consumer's complaint. The email advises consumers to open and "print a hard copy of the complaint for your records in the upcoming investigation." Opening the attachment, however, triggers the download of malicious spyware.

The FTC warns that the bogus email is personalized and may include the consumer's name as well as the name and address of the consumer's business. The agency advises consumers not to open the attachment, to delete the email, and to empty the deleted items folder.

The FTC's press release regarding this matter is available at: <http://www.ftc.gov/opa/2007/06/email.shtm>.

Additional information regarding how consumers can protect themselves from spyware and other cyber crime is available from a site sponsored by the FTC and other federal agencies: <http://onguardonline.gov/spyware.html> and <http://onguardonline.gov/phishing.html>.

- **Mass-Targeted Email Scam Reported** – Security vendor MessageLabs reported the first known "mass-targeted malicious-software attack." On June 26, MessageLabs intercepted more than 500 individual emails that targeted individuals who hold senior management positions in numerous organizations worldwide. The emails at issue included the name and job title of the victim in the subject line and an executable file embedded in a Microsoft Word document. If the target opened the document and clicked on a link, the file would run a data-stealing Trojan horse. The emails were designed to indirectly gain access to confidential correspondence and intellectual property in the possession of the recipient. The majority of the emails were sent to executives in the banking and finance sector, with chief investment officers targeted in 30 percent of the attacks. A spokesperson for MessageLabs stated that the hackers may have harvested the necessary information for the attack from search and social-networking sites.

An article about this development is available at: http://news.zdnet.com/2100-1009_22-6194497.html.



IV. SPAM

- **Plaintiff Wins Appeal for Claims Brought Under Washington Anti-Spam Law** – After a long fought battle, Washington state resident Joseph Hylkema may finally receive an award for spam emails that were sent to him in violation of Washington's anti-spam law. In March 2002, after receiving at least nine unsolicited email messages offering credit counseling services, Hylkema successfully obtained a default judgment of \$31,575 from a Washington state court under Washington state's plaintiff-friendly, anti-spam law. The alleged spammer, Credit Counseling Foundation of Fort Lauderdale, Florida, did not appear in the Washington court to defend itself from the lawsuit. After obtaining the judgment, Hylkema filed a second suit in a Florida court. At that point, Credit Counseling finally appeared and maintained that it did not send violative emails. The Florida trial judge rejected the company's defense. After navigating the appeals process, on June 13, a Florida appeals court ruled in Hylkema's favor and found that the Washington court had personal jurisdiction over Credit Counseling and upheld the ruling.

As noted above, Washington state had at the time a generous anti-spam law under which most people can sue for \$500 in damages per unsolicited message, and "interactive computer services" (which Hylkema claimed to be) can obtain \$1,000 in damages per message. Following the passage of CAN-SPAM in 2003, much of Washington's email law (including the damages portion) was preempted, and thus would be moot to current plaintiffs.

An article about this development is available at: http://news.com.com/2100-1030_3-6192208.html.

- **Electronic Service Allowed on Spammers With Inaccurate WHOIS Data** – In an "unpublished" decision, a U.S. District Court for the Northern District of California held that defendants charged with unsolicited commercial emailing may be served via email when the physical location information they have provided to WHOIS is incomplete or inaccurate. See *Balsam v. Angeles Tech. Inc., N.D. Cal., No. C06-04114, 6/6/07*.

The issue arose when plaintiff Daniel Balsam received an email allegedly in violation of California's anti-spam law. He was unable to serve summons on the defendants with the information available on the Whois registries. The court granted Balsam's petition to serve the defendants via email, subject to the stipulation that Balsam provide the email addresses that would be used to serve the defendants.

The text of the opinion is available at: <http://pub.bna.com/eclr/06cv04114.pdf>.

- **First Jury Convicted Spammer Sentenced** – Jeffrey Goodin, the first person ever convicted by a jury under CAN-SPAM, has been sentenced to 70 months in federal prison for targeting America Online (AOL) customers as part of an identity theft scheme.



See *United States v. Goodin, C.D. Cal., CR 06-186B, sentencing 6/11/07*. Goodin was also ordered to pay more than \$1 million to the victims of his phishing scheme, including almost \$1 million to Earthlink. As reported in an earlier edition of the *Privacy and Data Security Briefing*, the evidence suggested that Goodin used several compromised Earthlink accounts to send the fraudulent emails to AOL users. The messages appeared to come from AOL's billing department and urged users to update their billing information or else lose service.

An article about this development is available at: <http://pubs.bna.com/ip/BNA/EIP.NSF/7c407ecc8216ce4185256d05005e8b30/d60bf76dafbb092852573050073d43e?OpenDocument>.

- **Intent to Send Sufficient for CAN-SPAM Injunctive Relief** – A U.S. District Court for the Western District of Washington held that injunctive relief under CAN-SPAM may be awarded as long as a party intends that commercial emails be sent on its behalf. The party does not need to have knowledge that the commercial emails violate CAN-SPAM. See *United States v. Impulse Media Group Inc., W.D. Wash., No. CV05-1285, 6/8/07*.

Under CAN-SPAM, one who “initiates” the transmission of a commercial email that violates CAN-SPAM may be held liable for injunctive relief. See 15 U.S.C. § 7702. Under the act, “initiate” means “to originate or transmit [a] message or to procure the origination or transmission of such message.” “Procure” is defined as “intentionally . . . pay[ing] or provid[ing] other consideration to, or induc[ing], another person to initiate such a message on one’s behalf.” The Judge in *Impulse Media* concluded that this language imposed only an initiation requirement for injunctive relief and that the requisite initiation is satisfied whenever a party intentionally induces another to send the commercial email on its behalf. Knowledge is required for criminal penalties.

In the case at issue, plaintiff alleged that defendant procured the transmission of improper emails by the offending emailers. Defendant Impulse Media acknowledged that it intended the affiliates with which it contracted to “refer customers to its websites” but maintained that these companies were to generate these referrals through its affiliates’ own websites, and not through the use of commercial e-mail. In support of its position, defendant relied upon its explicit prohibition in its contract against unlawful commercial emails. Ultimately, after establishing that the plaintiff must demonstrate that a defendant intentionally induced its sending of commercial e-mails (without imposing an additional knowledge requirement for injunctive relief), the Judge concluded that there were disputed questions of material fact as to the defendant’s intent to send the commercial emails, and that the question of defendant’s intent was an issue for the fact finder at trial.

The court’s opinion is available at full text at <http://pub.bna.com/eclr/051285.pdf>.



V. TELECOM/WIRELESS

- **EPIC to Propose CPNI Regulations for Handset Makers** – In a first-of-its-kind proposal, the Electronic Privacy Information Center (EPIC) announced on June 28, 2007, that it will petition the FCC to expand its Customer Proprietary Network Information (CPNI) rules to manufacturers of telephone handsets. Today these regulations apply only to providers of telecommunications and VoIP services.

EPIC’s anticipated proposal follows in the wake of the FCC’s issuance of new rules earlier this year designed to protect consumers from pretexting and other types of data breaches—rules that were the direct result of a prior EPIC petition criticizing the FCC’s rules for not sufficiently protecting consumers from pretexting. Apparently, EPIC’s most recent concern stems from the fact that consumers selling handsets and related equipment on secondary markets such as eBay do not always successfully remove their private information from the devices prior to the sale.

It is not yet clear whether EPIC will seek FCC action through the FCC’s pending further rulemaking on CPNI or whether EPIC will file an entirely new petition. Also unclear is precisely what requirements EPIC will ask the FCC to impose on handset makers.

- **Senate Commerce Committee Passes Anti-Spoofing Measure** – On June 27, 2007, the Senate Commerce Committee approved S.704, the “Truth in Caller ID Act,” which would make it unlawful for anyone other than law enforcement to transmit misleading or inaccurate caller ID information. The bill is now expected to head to the full Senate for consideration.

Earlier this year (on May 24, 2007), the Senate Judiciary Committee considered and reported out a similar measure, H.R. 740, the “Preventing Harassment through Outbound Number Enforcement (PHONE) Act,” which had originated and was passed by the House Judiciary Committee as well. On June 19, 2007, Senator Kyl (R-AZ) introduced a related measure, S.1654, which would prohibit the sale or provision of caller ID spoofing services. The House Commerce Committee, for its part, considered and approved its own anti-spoofing measure, H.R. 251, the “Truth in Caller ID Act,” on June 11, 2007.

It is not clear yet which, if any, of these measures will become law. Congress clearly is interested in the issue, and the provisions in the various bill are materially similar.

Copies of S. 704, H.R. 740, S. 1654, and H.R. 251 can be found at: <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:s.00704>, <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.00740>, <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:SN01654:@@L&summ2=m&> and <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.00251>, respectively.

- **FCC Imposes \$9000 Fine for Transmission of Two Commercial Faxes** – On June 27, 2007, the FCC imposed a fine of \$9000 on a printing and copy supply company for



transmitting two unsolicited commercial faxes in violation of the Telephone Consumer Protection Act, the Junk Fax Prevention Act, and related FCC rules. According to the FCC, Tri-State Printer & Copier Co., Inc. was liable for this amount because it transmitted via fax at least two “unsolicited advertisements” absent consent or an established business relationship with the fax recipients. Apparently, Tri-State failed to respond to an FCC-issued citation that warned of the company’s possible violations, and Tri-State continued to transmit unsolicited commercial faxes even after it received the citation. Although the FCC is authorized to impose fines of as much as \$11,000 per offense, the FCC determined that it would impose the base level fine it previously used in commercial fax cases (\$4500) for each violation.

A copy of the FCC’s Notice of Apparent Liability for Forfeiture can be found at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-07-2827A1.doc.

- **Verizon Wireless Sues Telemarketers for Prerecorded Messages** – On June 19, 2007, Verizon Wireless announced that it filed a lawsuit against several Miami-based entities alleged to have transmitted prerecorded messages to subscribers promoting vacation and travel services. Verizon Wireless claims that nearly 900,000 calls were made to its subscribers in violation of, among other provisions, the Telephone Consumer Protection Act (TCPA), which bars the transmission of autodialed or prerecorded calls to mobile phones absent consent. Among the allegations is that the calling parties manipulated caller ID information to make it appear that their calls were coming from Kentucky, rather than Florida. The TCPA provides for damages in the amount of \$500 per violation, or three times that amount for conduct that is willful or knowing.

VI. GENERAL CONSUMER PROTECTION

- **Washington State Attorney General Announces Settlement with Companies that Offered Consumers “Free” Gifts** – On June 21, Washington State Attorney General Rob McKenna announced a settlement with the operators of www.privasafe.com and www.surfsafeinternetservices.com. The defendants advertised on their websites that they would protect consumers’ computers and privacy and shield them from unscrupulous marketers. The Attorney General alleged that the defendants instead sold consumers’ personal information and billed them for services they did not want or receive. The Attorney General further alleged that the defendants “lured” consumers with online offers for “free” gift cards and merchandise presented in pop-up and banner advertisements as well as in emails. Consumers submitted their personal information in order to receive the “free” products. However, the bottom of defendants’ web page, which could be viewed only by scrolling down, stated that individuals who completed the form would be charged and that only those who paid the \$14.95 monthly fee and remained in good standing for 90 days would receive the “free” item. The Attorney General stated that only one Washington consumer received the “free” item.

As part of the consent decree, which was filed in King’s County Superior Court in Washington, the defendants agreed to pay \$100,000 in civil penalties, \$200,000 in



attorneys’ fees, and to provide full refunds to Washington consumers who were billed for Privasafe or Surfsafe Internet services any time since January 1, 2004. The defendants agreed to notify eligible consumers by email and mail. Defendants also agreed not to sell or share any of the information collected from Washington consumers since January 1, 2004; to clearly and conspicuously disclose the terms of any offer for “free” items; and to not use a pre-checked box to indicate a consumer’s agreement to be billed for a product or service.

This is one of the first cases to address “free” offers that are prevalent on the Internet. The case combined several egregious facts, including that consumers were billed for services they never received, only one consumer appears to have received the promised “free” item, and consumers’ personal information was sold to marketers in spite of the defendants’ promise to protect consumers’ from unscrupulous marketers. Companies and marketers that provide such “free” offers should clearly and conspicuously disclose the terms of the offer as well as the fact that consumers’ personal information may be shared.

The Attorney General’s press release and a link to the complaint and consent decree are available at: <http://www.atg.wa.gov/pressrelease.aspx?id=16092>.

- **Association of National Advertisers Urges the FTC Not to Modify Endorsement Guides** – In response to a request for public comments regarding the FTC’s Guides Concerning the Use of Endorsements and Testimonials (the Guides), the Association of National Advertisers (ANA) filed comments with the FTC urging it to keep the Guides without modification. Currently, the Guides allow marketers to use testimonials that are not generally representative of what consumers can expect from the advertised product if the marketer clearly and conspicuously discloses (1) what the generally expected experience is in the depicted circumstances, or (2) that the depicted results are not representative or typical. According to the ANA, the FTC has suggested a change to the Guides that would require marketers to (1) conduct pre-publication proof of “generally expected results,” and (2) to disclose the typical experience a consumer could expect to have. As discussed previously in the *Privacy and Data Security Briefing*, the FTC is conducting a review of the Guides and as part of such review, issued a request for public comments in January 2007. We will continue to monitor the progress and outcome of the FTC’s review.

An article on this issue is available at: http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticle&art_aid=62575.

The ANA’s comments are available at: http://www.adlawbyrequest.com/_db/_documents/Comments_submitted_by_ANA.pdf.



VII. RADIO FREQUENCY IDENTIFICATION TECHNOLOGIES (RFID)

- **Senate RFID Bills Move Through the California Assembly** – The California Assembly Committee on the Judiciary recently passed five Senate bills seeking to regulate the use of RFID in identification documents, driver's licenses, school settings, and subcutaneous implants, and to impose consumer disclosure requirements when documents contain RFID technologies that hold personal information. As previously reported in the April 16 and June 4 *Privacy and Security Report Briefings*:
 - SB 28, introduced by Joe Simitian (D), would place a moratorium on the Department of Motor Vehicles' use of RFID in driver's licenses and ID cards.
 - SB 29, introduced by Joe Simitian, would place a moratorium on the use of RFID technologies in public schools for the purpose of recording student attendance or otherwise monitoring students' whereabouts while on school grounds.
 - SB 30, introduced by Joe Simitian, would, among other things, set basic standards for the use of RFID in government documents.
 - SB 362, introduced by Joe Simitian, would prohibit a person from requiring, coercing, or compelling another person to undergo a subcutaneous implant of an RFID device that transmits personal information.

In addition to the above, SB 388, introduced by Ellen Corbett (D), would require any private entity that sells, furnishes, or otherwise issues a card or other item containing a RFID tag to make certain disclosures to the recipient card- or item-holder.

Passage by the Assembly Judiciary Committee is but one of many steps involved in the California legislative process and, as such, none of the bills is a sure bet at this time for ultimate passage into law. Each bill must still work its way through the Assembly, which, in some instances, includes referrals back to committees for consideration, and passage by the Assembly floor. Additionally, if the bills are passed with amendments and, thus, are different from the Senate version, they will need to be sent to a conference committee where representatives from the Assembly and Senate will iron out the differences. If the bills pass through conference, they must then be passed by both houses and sent to Governor Arnold Schwarzenegger (R) for action.

Notably, SB 30 is very similar to a bill that passed both houses in 2006 (SB 762), but was vetoed by the Governor who said the bill was premature. SB 362 reportedly has bipartisan support and no apparent formal opposition and, accordingly, it holds some promise of making its way to the Governor's desk. The other bills face significant opposition from banking, retail, business associations, RFID manufacturers, and other technology companies, which generally take the position that the risks the bills seek to minimize are exaggerated, and the prohibitions on the use of the technologies will chill innovation.



Copies of the bills discussed above can be found at:

http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_362&sess=CUR&house=B&author=simitian.

http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_28&sess=CUR&house=B&author=simitian.

http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_29&sess=CUR&house=B&author=simitian.

http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_30&sess=CUR&house=B&author=simitian.

http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_388&sess=CUR&house=B&author=corbett.

July 10, 2007 – July 23, 2007.

I. PRIVACY

- **Bank of America Settles Class Action Lawsuit Alleging Privacy Violations** – Bank of America recently agreed to settle a class action lawsuit alleging that it engaged in “unlawful, unfair and fraudulent” business practices over a period of several years by “disclosing consumers’ personal, private, confidential information to third parties without consumers’ consent or without making proper disclosure.” Specifically, the lawsuit alleged that Bank of America disclosed its customers’ Social Security numbers, account numbers, and other sensitive data to third parties, including telemarketers and direct mail marketers, despite promises in its privacy policy to “keep the information you provide us secure and confidential” and to share customer information “only for legitimate business purposes.”

Bank of America denied allegations of wrongdoing, stating that it chose to enter the settlement in order to save costs over the long term. The settlement provides for \$10.75 million to go to waiving fees for certain bank products and services and to paying for several months of a credit-monitoring service; \$3.25 million will go to various privacy-related programs and consumer groups. Approximately 35 million Bank of America customers are eligible to participate in the settlement.

Bank of America's privacy policy now states that credit card customers' information may be shared with joint marketing partners and provides a number that consumers may call to opt out of such information sharing. This settlement highlights the importance of having clear and explicit policies regarding data collection and sharing practices. Regardless of whether a company might be able to prevail in court on the



merits of its privacy practices, the threat of prolonged litigation may be too much to bear. Making sure that consumers are aware of privacy practices upfront is crucial.

An article on this issue is available at: <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/07/11/BUG34QU38U1.DTL>.

- **U.S. House Subcommittee Plans Hearing into Google-DoubleClick Merger** – Representative Bobby Rush (D-IL), chairman of the House Subcommittee on Commerce, Trade and Consumer Protection, sent a letter to FTC Chairman Deborah Platt Majoras in connection with Google's proposed acquisition of DoubleClick. Representative Rush stated that the Subcommittee plans to schedule a hearing into the matter after Congress returns from its August recess and that there are concerns regarding competition and consumer privacy.

An article on this issue is available at: <http://www.internetnews.com/business/article.php/3689841>.

Representative Rush's press release is available at: http://www.house.gov/apps/list/press/i101_rush/rushgoogleletter.html

- **Google Plans to Shorten the Lifespan of its Cookies** – Google announced that “in the coming month” it will begin to issue cookies that expire two years after a user visits its website but will be updated each time a user returns to the website. Google's cookies are currently set to expire in 2038. Privacy experts praised Google's ability to evaluate and change its privacy practices, while noting that the policy is not likely to have a large impact on the amount of information Google is able to store about its users.

An article on this issue is available at: http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2090502.ece.

II. SECURITY

- **FTC Official Describes Commission Approach in Data Breach Investigations** – At a July 18 International Association of Privacy Professionals (IAPP) KnowledgeNet Brown Bag, Joel Winston, the FTC's Associate Director of the Division of Privacy and Identity Protection, confirmed that the FTC continues to investigate data breaches and has a number of ongoing cases. He acknowledged that, in the absence of a comprehensive data breach law, the Commission has adopted basic “objective” principles that guide their data breach investigations and enforcement activities. Winston stressed that the FTC has rejected inflexible technical standards for securing data and supports general principles that can be adapted for businesses and their particular data risks. In particular, he indicated that the FTC has used the Gramm-Leach-Bliley's (GLB) Safeguard Rule as the backdrop for evaluating a company's security procedures – although he emphasized that



compliance with the specific GLB rules was not required for non-GLB institutions, and instead GLB serves as a “rule of thumb” or general approach for companies that hold sensitive personal information data. Generally, Winston explained that under this standard, companies should:

- identify and assess the risks to personal information, and evaluate the effectiveness of the company's existing safeguards for controlling these risks;
- design and implement a safeguards program, and regularly monitor and test it;
- select service providers that can maintain appropriate safeguards, ensure that contracts with those service providers require them to maintain safeguards, and oversee their handling of customer information; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the company's business or operations, or the results of security testing and monitoring.

Winston also noted that the Commission has closed investigations in instances where companies had adopted appropriate data security safeguards. He indicated that FTC enforcement actions in the area of data security can be expected in the near future.

- **House Committee Approves Bill Restricting the Sale and Use of Social Security Numbers** – The House Ways and Means Committee unanimously approved H.R. 3046, which would prohibit the sale, purchase, or public display of Social Security Numbers (SSNs). The statute defines SSNs to include any derivative of the number, such as the last four digits. The bill contains several exceptions relevant to private sector entities, including purchase or sale to or from a Consumer Reporting Agency pursuant to a permissible purpose under the Fair Credit Reporting Act. These permissible purposes primarily relate to offering consumer credit or insurance products. The bill would not allow the purchase or sale of SSNs for marketing or fraud prevention purposes.

The bill would also prohibit companies from including SSNs on employee badges (whether printed on the card or embedded on the magnetic stripe) and printing SSNs on checks or documents accompanying checks. Businesses would also be required to restrict access to SSNs to employees that had a legitimate need for the data.

The Ways and Means Committee approved a similar bill in 2004, but it failed to pass the full House. The Senate is considering a similar bill, S.238, which was introduced by Senator Dianne Feinstein (D-CA).

Even in the absence of federal legislation, at least 24 states already have some restrictions on the use or sale of SSNs.

A copy of H.R. 3046 is available at: http://thomas.loc.gov/cgi-bin/t2GPO/http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h3046ih.txt.pdf.



- **Data Breach by IT Employee** – In the last two weeks, at least five new data breaches have been reported in the media. One breach, at Certegey Check Services, highlights the importance of internal controls and employee screening. A senior database administrator at Certegey downloaded 2.3 million records containing personal information, including names, addresses, birth dates, and bank account and credit card numbers and sold the data to a marketing firm. Customers reported receiving marketing material as a result of the breach and Certegey is in the process of notifying all affected customers. The employee was of course fired and Certegey has filed a civil suit against the employee and the marketing firm.

An article on this issue is available at:

http://today.reuters.com/news/articleinvesting.aspx?type=comkktNews&rpc=33&storyid=2007-07-03T180045Z_01_N03180178_RTRIDST_0_FIDELITYNATIONAL-IDENTITYTHEFT-UPDATE-3.XML

- **DOJ Proposes ID Theft Law** – The Department of Justice has submitted to Congress the *Identity Theft Enforcement and Restitution Act*, which would update and increase the penalties in current ID theft statutes. The most important change for businesses is the inclusion of the theft of corporate identity as an offense. The current law only addresses the theft of an individual's identity.

A press release discussing the proposed legislation is available at:

http://www.usdoj.gov/opa/pr/2007/July/07_ag_521.html

III. SPAM

- **New Kit Makes Phishing Easier** – The rise in phishing scams has been widely reported, and now such scams are even easier to perpetrate. RSA's Anti Fraud Centre reports that fraudsters have developed a "plug-and-play" phishing kit that can be installed within two seconds and can be easily installed to create fake banking web sites. The kit consists of a single file that can create an operational phishing site on a compromised server with the click of a mouse. The software automatically creates the relevant directories and installs all the necessary files to create a fake site, including HTML pages and company logo images. The system also decreases the risk of being identified by PC and network security systems, because it only accesses a host server once to create a phishing site.

To date, the kit is only known to have been used to attack one financial institution, but RSA expects that it will be used by others in the future. Banks, financial institutions, and other websites should be on the alert for more phishing scams, and warn customers to be cautious when providing their personal information online.

An article about this development is available at:

<http://www.vnunet.com/computing/news/2194016/phishing-made-easy-fraudstrs>



IV. TELECOM/WIRELESS

- **Rhode Island Commercial Fax Bill Goes Into Effect** – Rhode Island's commercial fax bill, SB 191, recently went into effect. The new law allows recipients of unsolicited commercial faxes to sue senders for \$500 per message, up to a maximum of \$50,000 in damages. The law also authorizes the Rhode Island Attorney General to aggregate complaints against a sender and prosecute those complaints via a class action lawsuit. Now that Rhode Island has enacted its own commercial fax law, commercial faxes that are transmitted to consumers in Rhode Island could be subject to both state and federal penalties.

Additional information about SB 191, including the text of the bill, is available at:

<http://dirac.rilin.state.ri.us/BillStatus/WebClass1.ASP?WCI=BillStatus&WCE=ifrmBillStatus&WCU>

- **FCC Imposes Fines For Single Violation of Commercial Fax Rules; Fines Also Levied for Multiple Commercial Fax Transmissions** – On July 23, 2007, the FCC imposed a fine of \$4,500 against each of Aras Marketing, Inc. ("Aras") and Global QA Corp. ("Global QA") for transmitting just one unsolicited commercial fax in violation of the Telephone Consumer Protection Act, the Junk Fax Prevention Act, and related FCC rules. Although the FCC has used \$4,500 per violation as a standard base forfeiture amount for such infractions (it is authorized to impose fines of as much as \$11,000 per offense), it generally has proposed and issued forfeitures only for multiple infractions. To our knowledge, these cases mark the first instances in which the FCC has proposed a fine for a single violation of the commercial fax rules. Apparently, Aras and Global QA each failed to respond to FCC-issued citations warning them of possible violations based on the FCC's receipt of one or more complaints (the FCC did not specify how many complaints). When each company subsequently transmitted a single commercial fax in violation of the rules and resulting in a consumer complaint, the FCC took action.

The FCC also recently imposed fines of \$13,500 (against ESPEED Mortgage Dot Com, LLC ("ESPEED")), \$22,500 (against Troeschler Typing Service ("Troeschler")), and \$13,500 (against CyberData, Inc. ("CyberData")) for similar commercial fax violations. Like Aras and Global QA, ESPEED, Troeschler, and CyberData each failed to respond to an FCC-issued citation warning about one or more possible violations and continued to transmit at least one unsolicited commercial fax after receiving the citation. Troeschler apparently transmitted five such faxes, while ESPEED and CyberData each transmitted three. The FCC imposed base level fines of \$4,500 for each violation.

Copies of the FCC's Notices of Apparent Liability for Forfeiture can be found at:

http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-07-3374A1.doc (Aras Notice);

http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-07-2749A1.doc (Global QA Notice);



http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-07-3372A1.doc (ESpeed Notice);
http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-07-3299A1.doc (Troeschler Notice);
http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-07-3282A1.doc (CyberData Notice).

- **FCC Imposes Fine For Single Violation of Prerecorded Message Rules** – On July 23, 2007, the FCC imposed a fine of \$4,500 against Travelcomm Industries, Inc. (“Travelcomm”) for delivering just one unsolicited, prerecorded advertising message in violation of the Telephone Consumer Protection Act and related FCC rules. Although the FCC has used \$4,500 per violation as a standard base forfeiture amount for such violations (it is authorized to impose fines of as much as \$11,000 per offense), it generally has proposed forfeitures only for multiple violations. Apparently, Travelcomm failed to respond to an FCC-issued citation warning the company about one or more possible violations. When it subsequently transmitted a single unsolicited, prerecorded advertising message and received a consumer complaint, the FCC acted and imposed the forfeiture.

A copy of the FCC’s Notice of Apparent Liability for Forfeiture can be found at:
http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-07-3375A1.doc.

V. GENERAL CONSUMER PROTECTION

- **Ninth Circuit Holds that Email Headers and IP Addresses Carry No Reasonable Expectation of Privacy** – *United States v. Forrester* was argued before the Ninth Circuit on January 12, 2007, and decided on July 7, 2007. The case involved two defendants, Forrester and Alba, who were convicted at trial for various offenses relating to the operation of a large Ecstasy-manufacturing laboratory. During its investigation of the defendants, the government employed various computer surveillance techniques to monitor Alba’s email and Internet activity. The surveillance began in May 2001 after the government applied for and received a “pen register analogue” on Alba’s computer. The only data obtained through this method were (1) the to and from addresses of Alba’s email messages, (2) the IP addresses of the websites that Alba visited, and (3) the total volume of information sent to or from his account.

Alba challenged his conviction on the ground that he had a reasonable expectation of privacy in this data, and that the government therefore conducted an illegal search by not first procuring a search warrant based on probable cause. The Ninth Circuit panel rejected these arguments, analogizing all three types of data to telephone pen register information (a pen register is a device that monitors a phone line and records a list of all calls made from that phone), the searching of which the Supreme Court held not to be a violation of the Fourth Amendment in *Smith v. Maryland*, 442 U.S. 735 (1979). The Supreme Court in *Smith* held that the use of pen registers without a warrant does not violate the Fourth Amendment because (1) the data is voluntarily transmitted to the phone company, a third party, and (2) the phone numbers captured merely constitute



“addressing information,” like information visible on the outside of an envelope, and do not reveal the contents of the phone communication, which are otherwise protected by the Fourth Amendment under *Katz v. United States*, 389 U.S. 347 (1967).

The panel analogized the data obtained in the search of Alba’s computer to that obtained by using pen registers. It held that email and Internet users have no expectation of privacy in the to and from addresses of their messages or the IP addresses of the websites they visit because “they should know that these message are sent and these IP addresses are accessed through the equipment of their Internet service provider and other third parties.” The Ninth Circuit also likened the government’s surveillance of email addresses to addresses on the exterior of physical mail, the search of which is also not a violation of the Fourth Amendment. It found that email, like a physical package, could be separated into two distinct portions – the addresses, which like those on a physical package are transmitted to a third party and are thereby searchable, and the contents, which are not searchable without a warrant.

In addition, the panel noted that this data revealed no more about the underlying contents of the communication than phone numbers discovered by the use of pen registers. With regard to emails, the panel noted that a search of to and from addresses does not include the contents of the messages, and is essentially no different than a search of numbers dialed from a particular telephone. With regard to the IP addresses of websites visited, the panel noted that such information does not include the particular pages on the websites the person viewed, and observed that at best the government can only speculate about what was viewed on the websites. The court emphasized that the government’s educated guesses about the contents of the emails or web pages is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed.

With regard to the third type of data recovered by the search – the total volume of information sent to and from the email account – the court held that the discovery of such information was incidental to the legal monitoring of the addressing information, and thereby did not breach the line between mere addressing and more content-rich information.

The Ninth Circuit panel distinguished IP addresses from URLs, noting that material after the domain name in a URL could reveal content as opposed to addressing information. The court also cautioned that its holding applied only to the particular data-gathering techniques used in the case at hand.

A copy of the Ninth Circuit’s decision is available at:
<http://pub.bna.com/eclr/0550410.pdf>.

- **AOL Settles with 48 States over its Cancellation Policies** – The Attorneys General of 48 states and the District of Columbia announced on July 11 that they had entered into a settlement with America Online Inc. (AOL) in connection with AOL’s customer



cancellation policies. The investigation and settlement arose out of customer allegations that after AOL changed from a subscription-based to a free service, customers who attempted to cancel had difficulty doing so and were in some instances charged after they canceled. AOL noted that the investigation arose out of complaints involving less than .001 percent of total transactions at AOL. The states also alleged that AOL had misrepresented the terms and costs of its services. Under the settlement, AOL will pay \$3 million to the states and an unknown amount in refunds to consumers. AOL has also agreed to allow customers to cancel their service online, to restrict the practice of trying to “save” customers, to record and verify calls cancellation calls, and to provide improved disclosures to customers about fees and policies. AOL reached similar settlements with New York in 2005 and with the FTC in 2004.

A copy of the Assurance of Voluntary Compliance and a copy of the California Attorney General’s press release is available at: <http://ag.ca.gov/newsalerts/release.php?id=1435>.

- **FTC Issues Closing Letter to Social Networking Website Regarding COPPA Investigation** – The FTC released a closing letter dated May 17, 2007, which states that the FTC conducted an investigation into whether Bebo, Inc., a social networking website, had violated the FTC’s Rule implementing the Children’s Online Privacy Protection Act (COPPA). The letter further states that the FTC determined that no enforcement action would be recommended at this time. The letter does not go into detail regarding the conduct at issue, but it does state that COPPA, “[i]n pertinent part, . . . requires operators of websites directed to children under 13 years of age, or that have actual knowledge that they are collecting personal information online from such children, to provide notice of their information practices to parents and to obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children under 13.” In the letter the FTC reserves the right to take further action. As discussed in a previous issue of the *Privacy Briefing*, the FTC entered into a consent decree with, and obtained a \$1 million penalty from, Xanga, another social networking website, for alleged COPPA violations in September 2006.

A copy of the FTC’s closing letter is available at: <http://www.ftc.gov/os/closings/staff/070517BeboClosingLetter.pdf>.

- **Groups Ask FTC to Investigate Potential FCRA Violations by Transportation Employers** – A coalition of groups, including the Center for Democracy and Technology, Rainbow/PUSH, the National Workrights Institute, the Legal Action Center, and the National Employment Law Project, have filed a complaint with the FTC, requesting it to investigate railroad and other transportation employers who allegedly violate the Fair Credit Reporting Act (FCRA) by not providing employees with “clear and conspicuous” notice when conducting criminal background checks on them. The complaint alleges that employees were not told they were under investigation; were told that the background checks were required by the federal government when they were not; and/or received notice in English when they spoke only Spanish. The complaint further alleges that employees were not given access to their background checks and were not



notified why they were fired. This complaint raises interesting issues regarding the application of the FCRA in the context of background checks conducted by employers; we will monitor the FTC’s response.

An article on this issue is available at: <http://www.washingtonpost.com/wp-dyn/content/article/2007/07/11/AR2007071102205.html>.

VI. INTERNATIONAL AFFAIRS

Canada Federal Court Rules that Privacy Commissioner Has Jurisdiction to Investigate Trans-Border Flows of Canadians’ Personal Information – The Federal Court in Canada recently ruled that the Personal Information Protection and Electronic Documents Act (PIPEDA) gives the Privacy Commissioner jurisdiction to investigate trans-border flows of personal information. This ruling relates to a complaint that was filed with the Office of the Privacy Commissioner three years ago about a U.S. based website, Abika.com, that could provide background checks, telephone numbers, license plate numbers, psychological profiles, and other information about individuals, including Canadians. The Office of the Privacy Commissioner determined that it was unable to investigate the website, based on lack of jurisdiction in the U.S., based on an assessment that the website did not provide Canadian-based sources and was not substantially connected to Canada. The impact of this decision is important with regard to enforcement of Canadian citizens’ privacy rights and protections, due to the definitive finding that the Privacy Commissioner is not restrained from investigating cross-border data transfers. The Office of the Privacy Commissioner issued a statement about the ruling, stating in part, that “We will take guidance from the court. We’re very pleased with the decision that gives us the jurisdiction to investigate the matter. The issues surrounding data flow are important to this Office.”

A detailed article of the facts and background on this ruling is located at: <http://rs6.net/tn.jsp?t=hp48lccab.0.fdjmmccab.f9ki7zaab.1370&ts=S0259&p=http%3A%2F%2Fwww.itbusiness.ca%2Fit%2Fclient%2Fen%2FHome%2FNews.asp%3Fid%3D42148>.

EU – SWIFT Joins U.S. Safe Harbor to Allow for Data Transfers from the EU to the U.S. for Anti-Terror Probes

On July 19, 2007, SWIFT, the Society for Worldwide Interbank Financial Telecommunication, a cooperative owned by over 8,100 customer financial institutions in 207 countries and territories to facilitate international transactions, joined the U.S. Department of Commerce’s Safe Harbor Program. This action will allow U.S. anti-terror authorities to use SWIFT’s database in its investigations, while confirming adequate protection of the privacy rights of EU citizens. Under the Safe Harbor Program, SWIFT must guarantee that customer data stored in its U.S. operating center are treated in accordance with and protected under EU data protection laws. In addition to its new Safe Harbor status, SWIFT introduced two new policies, a data retrieval policy and a personal



data protection policy. "These combined actions reinforce legal certainty for SWIFT and the international financial community, and ensure further compliance with their respective obligations under European data protection law," SWIFT said in a July 20th news release.

SWIFT's Safe Harbor registration is available at:

<http://web.ita.doc.gov/safeharbor/SHList.nsf/f6cfd20f4d3b8a3185256966006f7cde/53a98f15c156d3b08525731d007381f3?OpenDocument&Highlight=2,SWIFT>

July 24, 2007 – August 14, 2007.

I. PRIVACY

- **Search Engines Announce Privacy Changes** – Following Google's announcements that it would delete cookies after two years of inactivity and modify search logs after 18 months so that they could not be tied to individuals (both announcements were discussed in previous issues of the *Privacy and Data Security Briefing*), Ask.com, Microsoft, and Yahoo have each announced changes to their privacy practices.

Microsoft announced new steps to protect users' privacy including, making search query data anonymous after 18 months by permanently removing cookie IDs, the entire IP address, and other identifiers from search queries; providing users the ability to opt out of behavioral ad targeting by its network advertising service; and joining the Network Advertising Initiative later this year.

Yahoo announced that it will remove portions of IP addresses and personally identifiable cookie IDs within 13 months unless users want the data retained for longer or the company is required to retain the data longer for legal reasons.

Ask.com will introduce a new tool called AskEraser that will allow users to search anonymously by choosing not to allow the search engine to retain user data during a search. For users that do not choose this option, Ask.com will disassociate search terms from the IP address after 18 months.

Microsoft and Ask.com have also called for the search industry to develop better privacy principles for the collection, use, and protection of data. They have proposed a meeting of leading search providers, online advertising companies, and privacy advocates to discuss these issues. Privacy advocates are heartened at the move toward better privacy practices but are also somewhat skeptical as to the actual impact of some of the announced changes.

In related news, the Center for Democracy and Technology published its Search Privacy Practices report, setting forth and comparing the revised privacy policies of the five



largest search providers, as well as giving recommendations as to how to further strengthen privacy protections.

Articles on this issue are available at:

http://news.com.com/Search+engines+race+to+update+privacy+policies/2100-1030_3-6198053.html?tag=nefd.top; <http://www.vnunet.com/vnunet/news/2194762/microsoft-ask-google-privacy-search>; <http://www.peworld.com/article/id,135075-c,yahoo/article.html>; and <http://www.peworld.com/article/id,135316-c,onlineprivacy/article.html>.

A press release announcing the CDT's report is available at:

<http://cdt.org/press/20070808press.php>.

The CDT's full Search Privacy Practices report is available at:

<http://www.cdt.org/privacy/20070808searchprivacy.pdf>.

- **FTC to Host Town Hall Meeting to Discuss Online Advertising Practices** – The FTC has announced that it will host a two-day "town hall" meeting to address the consumer protection issues raised by online advertising practices. The meeting will take place November 1-2, 2007 and is intended to bring together consumer advocates, industry representatives, technology experts, and academics. Interested parties are invited to submit requests to be panelists and to recommend topics for discussion.

The FTC press release announcing the meeting is available at:

<http://ftc.gov/opa/2007/08/ehavioral.shtm>.

- **Ninth Circuit Rules Online Contracts Cannot Be Changed Without Notice** – The U.S. Court of Appeals for the Ninth Circuit recently ruled that online changes to contracts (in this circumstance, terms of use) without notice to customers are not effective. The plaintiff in the case, Joe Douglas, sued Talk America Holdings Inc. (Talk America), alleging that after Talk America bought a business from AOL, Talk America changed the terms of use contract that AOL had had with its customers by adding an increase in prices, an arbitration clause, and a class-action suit waiver. Douglas was unaware of these changes for four years; when he became aware of the changes, he sued Talk America, alleging violations of the Federal Communications Act, breach of contract, and violations of other California consumer protection provisions. The Ninth Circuit found that companies cannot change materially their contracts and post those changes on their website without notifying customers. The court also stated that "[p]arties to a contract have no obligation to check the terms on a periodic basis to learn whether they have been changed by the other side."

While this case does not squarely address privacy policies, it does raise the question of whether the common practice in privacy policies of making changes and stating that consumers should periodically review the privacy policy for any changes is sufficient. The case highlights that for material changes certainly, additional notice and in some cases, agreement to the changes, is encouraged and may be required.



An article on this issue is available at:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9028240&source=rss_news10.

The court's opinion is available at: http://pub.bna.com/eclr/0675424_071807.pdf.

- **Class-Action Lawsuit Filed Against USPS** – A class-action lawsuit alleging that the U.S. Postal Service (USPS) sold employees' personal information to marketing companies in violation of the U.S. Privacy Act has been filed on behalf of all postal service employees. The lawsuit alleges that the USPS allowed private marketing companies to access and use its employee master file, which contains personal information, including home addresses, of all USPS employees. The lawsuit seeks to enjoin the USPS from continuing to disclose employees' information and to recover the money the USPS made by sharing its employees' information.

An article on this issue is available at:

<http://www.informationweek.com/news/showArticle.jhtml?articleID=201201888>.

II. SECURITY

- **House Committee Holds Hearings on Risks of P2P Programs** – The House Oversight and Government Reform Committee held a hearing to discuss the potential risks of P2P file-sharing programs and to consider if legislation is necessary to address the problem. The hearings were triggered in part by a study released in March by the Patent and Trademark Office that found that file-sharing networks continue to expose consumers' personal data. A committee spokesman confirmed, however, that legislative action was not imminent.

Mary Koelbel Engle, Associate Director for Advertising Practices at the Federal Trade Commission, testified that the FTC had addressed file-sharing concerns in the past through hearings, consumer and business education and two enforcement actions, but was considering reviewing industry practices again in light of the PTO report.

P2P file sharing software has been blamed for one recent data breach. Pfizer announced in June that 17,000 employee records were compromised when an employee's spouse downloaded file sharing software onto a company laptop. Most of the records, which included names and Social Security Numbers, were accessed and copied by an unknown number of users of the P2P network. The breach is being investigated by the Connecticut Attorney General.

More information about the hearing including Congressman Waxman's statement and testimony from most panelists is available at: <http://oversight.house.gov/story.asp?ID=1424>.

- **FTC Seek Comments on the Uses of Social Security Numbers** – The FTC is seeking comments on how the private sector uses Social Security Numbers ("SSNs"), the benefits, such as authentication and fraud prevention, and the risks, including identity theft. The request for comments is driven by a report issued by the President's Task



Force on Identity Theft which recommended various federal agencies develop a comprehensive record on the uses of SSNs in the private sector and evaluate the necessity of those uses. Comments are due September 5, 2007.

At least 24 states already restrict private sector use of Social Security Numbers. In addition, as reported in the July 25 *Privacy and Data Security Briefing*, the House Ways and Means Committee has approved H.R. 3046, which would prohibit the sale, purchase and public display of SSNs. No further action has been taken on that bill.

The FTC's Request for Comments and instructions for submitting comments is available at: <http://www.ftc.gov/opa/2007/07/ssncomments.shtm>.

III. SPAM

- **Court Rejects Corporate Officer's Motion to Dismiss CAN-SPAM Claims Against Him** – The U.S. District Court for the Western District of Washington rejected a motion to dismiss filed by a defendant officer and director of a corporation that was also sued under CAN-SPAM. See *Omni Innovations LLC v. Impulse Mktg. Group Inc., W.D. Wash., No. C06-1469, 7/18/07*. The plaintiffs in the case, which include the owner of and Internet Service Provider (ISP) and a customer e-mail account holder of the ISP, filed a complaint alleging that they received unsolicited e-mails from the corporate defendant, Impulse, a Nevada corporation. In connection with these allegations, the plaintiffs brought CAN-SPAM and related Washington state law claims against Impulse as well as Jeffrey Goldstein—a Georgia resident, officer, director, and majority shareholder of Impulse.

Notably, the court rejected Goldstein's motion to dismiss, which was grounded upon a lack of personal jurisdiction. The court concluded that Internet contact was sufficient to meet the standard for specific jurisdiction under Washington's long-arm statute and that Goldstein purposefully committed an act by transmitting e-mails to domains and e-mail accounts in Washington. The court also rejected Goldstein's argument that the plaintiffs failed to state a claim against him because they could not pierce the corporate veil. The court held that because Goldstein was a corporate officer, under Washington law, he could be held liable without piercing the corporate veil.

On the substance of plaintiff's claims, Goldstein moved to dismiss the complaint because plaintiffs alleged only that Goldstein "assisted" in the transmission of illegal e-mails which, Goldstein contended, is not a viable claim under CAN-SPAM and the related state law. The court disagreed and held that CAN-SPAM's prohibition on "initiating" also encompassed a prohibition against assisting in such activity.

A copy of the court's opinion is available at: http://pub.bna.com/eclr/06cv01469_071807.pdf.

- **Spammers Turn to Excel Spreadsheets and PDF documents to Send Spam** – E-mail security vendor Commtouch Software Ltd. reports that spammers are using Microsoft Excel spreadsheets to spread their e-mails and avoid antispy filters. The reported spreadsheets contain unsolicited messages that contain the familiar fraudulent stock tips



seen in traditional spam. Commtouch states that this development is “a natural progression after the recent spate of PDF spam” and that other file formats are likely to follow. Presumably, as spam filters develop ways to combat these new file formats, legitimate e-mails containing spreadsheets could get caught in the trap.

An article about this development is available at:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&%20taxonomyId=9&articleId=9027942&intsrc=hm_topic.

IV. SPYWARE

- **FTC Testifies on Peer-to-Peer File Sharing Risks** – Mary Engle, Associate Director of the FTC’s Division of Advertising Practices, testified before the House Committee on Oversight and Government Reform on July 24, 2007 regarding the risks associated with peer-to-peer (P2P) file sharing and the FTC’s efforts to mitigate them. In her testimony, Ms. Engle noted that the use of P2P file sharing poses a myriad of consumer risks including exposing consumers’ computers to spyware; exposing consumers to civil and/or criminal lawsuits from parties enforcing copyright and pornography laws; and exposing consumers, especially children, to unwanted pornography.

Ms. Engle noted that the FTC was working to mitigate these risks through a number of FTC initiatives including working with industry to improve disclosure of risk information on P2P sites; taking legal action against particularly egregious P2P file sharing operations; and educating consumers and businesses about the potential risks associated with P2P programs including the provision of guidance regarding how consumers and businesses can best protect themselves.

The FTC’s press release regarding its testimony before the House Committee on Oversight and Government Reform is available at:
<http://www.ftc.gov/opa/2007/07/p2.shtm>.

The FTC’s prepared statement before the Committee regarding the risks associated with peer-to-peer file sharing is available at:
<http://www.ftc.gov/os/testimony/P034517p2pshare.pdf>.

V. TELECOM/WIRELESS

- **FCC Fines Companies \$10,000 for Egregious Violations of the Commercial Fax Law** – On July 31, 2007, the FCC proposed to fine Extreme Leads, Inc. \$1.38 million for unlawfully transmitting at least 218 unsolicited advertisements via facsimile to 132 consumers. The fine was based on the transmission of 146 commercial faxes at \$4,500 each, which is the standard base forfeiture amount for such violations, and an increased base forfeiture level of \$10,000 for 72 transmissions that were sent after consumers requested – or attempted to request – that Extreme Leads cease transmitting commercial faxes to them.
- On August 1, 2007, the FCC similarly proposed a fine of \$87,500 against MHJP, Inc., f/k/a BCJR, Inc. (“MHJP”), for transmitting seventeen unsolicited advertisements via facsimile to thirteen consumers. Once again, while the FCC imposed its standard base



forfeiture amount of \$4,500 for most of the transmissions, it increased that amount to \$10,000 where customers had specifically requested that MHJP cease sending such facsimiles.

The FCC also imposed a \$130,500 fine on August 1, 2007, against Red Rose International for unlawfully transmitting at least 29 unsolicited advertisements via facsimile to 18 consumers. The proposed fine in this case was based on the more typical base forfeiture amount of \$4,500 per transmission.

Copies of the FCC’s Notices of Apparent Liability for Forfeiture can be found at:

http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-131A1.doc (Extreme Leads)

http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-135A1.doc (MHJP)

http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-134A1.doc (Red Rose)

- **California Court of Appeals Upholds Trial Court’s Ruling that Exemption in Anti-Junk Fax Statutes Applies to Business-to-Business Marketing** – On August 2, 2007, a California Court of Appeals upheld a trial court’s ruling that the “established business relationship” exemption applies equally in both the telemarketing and commercial fax contexts to business-to-business marketing as well as business-to-consumer marketing. The Appellate Court’s conclusion in this case resulted in the upholding of a dismissal of a class action lawsuit filed against a fax transmitter.

The Court of Appeals opinion can be found at:
<http://www.courtinfo.ca.gov/opinions/documents/B187254.DOC>.

- **Senate Commerce Committee Approves Bill to Reauthorize Do Not Call Fees** – On August 2, 2007, the Senate approved legislation (S. 781) to reauthorize the collection of fees for the national Do-Not-Call Registry. The bill, adopted by unanimous consent, would permanently extend the FTC’s authority to collect registry fees from telemarketers under the Do Not Call Implementation Act. Absent Congressional approval (which is expected), the FTC’s authority to fund the program through telemarketer fees will expire at the end of 2007.

A copy of S. 781 can be found at: <http://thomas.loc.gov/cgi-bin/query/z?c110:S.781>.

- **FTC Pursues Canadian Calling Card Telemarketers for Fraud** – On July 24, 2007, the FTC filed a civil lawsuit against a Canadian-based telemarketing company and two of its officers for fraudulent marketing of phone cards to U.S. citizens and for violating the National Do-Not-Call rules. The lawsuit, which was filed in the Northern District of Ohio, alleges that beginning in 2004, Quebec, Inc., called consumers posing as a bank or credit card company and offered a trial of long distance calling cards for \$1, but that consumers ultimately were charged more without notice and without ever receiving the cards. Quebec, Inc., also failed to pay the required fee to access the Registry and violated the Do-Not-Call laws by contacting consumers whose numbers appeared on the Registry.

More information about the law suit, including a copy of the complaint, can be found at:
<http://www.ftc.gov/os/caselist/0523081/index.shtm>.



- **Canadian Regulator Seeks National “Do Not Call” Registry Operator** – On July 30, 2007, the Canadian Radio-Television and Telecommunications Commission issued an RFP seeking an operator for its proposed new National Do-Not-Call Registry. The RFP seeks a contractor to develop, implement, and manage the Registry. Interested parties must show that they have the necessary financial resources, provide a company profile, and possess a “qualified management team” capable of developing and managing the Registry. The RFP will close on September 10, 2007, and the creation and implementation of the Registry is expected to follow soon thereafter.

Additional information about the RFP is available at:
<http://www.crtc.gc.ca/eng/NEWS/RELEASES/2007/r070730.htm>.

VI. CPNI

- **FCC Continues to Fine Carriers for Lack of CPNI Certifications** – On August 10, 2007, the FCC proposed to fine two carriers for their failure to produce certifications of compliance with the FCC’s Customer Proprietary Network Information (“CPNI”) rules, which address the treatment of confidential consumer calling data. Specifically, the FCC fined two carriers – Connect Paging, Inc., and Capital Telecommunications, Inc. – \$100,000 each for their failure to produce these certifications. The FCC also separately proposed to fine Connect Paging \$4000 for failing to respond to an FCC inquiry regarding CPNI compliance in a timely manner. The FCC proposed to fine a third carrier, PhoneCo, LP, \$4,000 for a similar infraction.

Copies of the FCC’s proposed forfeiture orders can be found at:

http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-07-3582A1.doc (Connect Paging);

http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-07-3584A1.doc (Capital); and

http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-07-3583A1.doc (PhoneCo).

VII. RADIO FREQUENCY IDENTIFICATION TECHNOLOGIES (RFID)

- **Federal Government Report Addresses RFID** – The National Institute of Standards and Technology (NIST), U.S. Department of Commerce, issued a 154 page report in April 2007 setting forth guidelines for securing RFID systems. According to the lead author – Tom Karygiannis – the report is intended to provide organizations and individuals, including hospitals and patients, retailers and customers, and manufacturers and distributors, practical ways to address the potential RFID security risks based on controls that are commercially available today.

Among other things, the report identifies some of the major business risks associated with implementing RFID technology, explains various RFID security controls, and provides recommendations for organizations using RFID systems to follow throughout the system’s life cycle. It also provides hypothetical case studies that illustrate how the concepts and recommendations provided in the guidelines could work in practice.



A major premise of the guidelines is that security controls should be incorporated throughout the entire life cycle of the RFID system – from initiation (e.g., pre-design) to disposition (e.g., retirement of system).

The report is available at http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf.

A recent article addressing the report is available at <http://www.technewsworld.com/story/58513.html>.

VIII. STATE ISSUES

- **New York Governor Spitzer vetoes three bills addressing elements of identity theft bills** – Governor Elliot Spitzer vetoes three identity theft bills on August 1, for a variety of reasons, despite claiming to agree in principle to many of the ideas. First, with regard to A. 217 – a bill that would create a Consumer Protection Board with subpoena power, Spitzer objected to the subpoena authority, said that it was not necessary to create such a board statutorily, and the proposed police power duplicated a bill passed previously this year (S. 5541). A. 61 did not allow companies to take “adverse actions” against “victims of identity theft”, but Spitzer found the language overly broad. A. 1108 echoed a theme that is starting to be addressed in many legislatures – limiting the use of Social Security numbers, this time with state employees. Spitzer thought the bill required the overhaul of several state infrastructures, therefore vetoed it. Nonetheless, this issue may be addressed in state and federal legislatures in the near future.
- **Texas Attorney General Abbott continues crusade against improper discarding of sensitive personal information** – General Greg Abbott filed suit against fitness company Lifetime Fitness for allegedly throwing away documents containing customers’ names, Social Security numbers, addresses, and credit card information behind Dallas-based clubs. The AG lawsuit alleges violations of the Texas Deceptive Trade Practices Act (DTPA) and the 2005 Identity Theft Enforcement and Protection Act. Abbott has brought several similar law suits against companies on the same basis, and clearly has been a focal point of his administration to date.

The Texas AG press release is available at:
<http://www.oag.state.tx.us/oagNews/release.php?id=2114>

IX. INTERNATIONAL AFFAIRS

Canada – Privacy Commissioner Issues Federal Guidelines for Dealing with Data Security Breaches – The Office of the Privacy Commissioner of Canada recently issued federal guidelines on dealing with data security breaches. While the guidelines are voluntary, they are meant to provide guidance to private sector organizations and assist them in responding when a privacy breach occurs. The guidelines provide four key steps to consider when responding to a breach or suspected breach: (1) breach containment and preliminary assessment, (2) evaluation of the risks associated with the breach, (3) notification, and (4) prevention. The guidelines emphasize that the decision how to



052 3148

respond should be made on a case-by-case basis. In addition, a Privacy Breach Checklist was released to supplement the guidelines and further assist organizations in assessing and responding to breach incidents. Privacy Commissioner Jennifer Stoddart still believes that there is a need for federal legislation, whether by amending PIPEDA or implementing new legislation, to compel businesses to notify individuals whose personal information has been accessed in an unauthorized manner but the guidelines should assist organizations to make well-reasoned and responsible decisions in responding to breach situations.

The guidelines, Key Steps for Organizations in Responding to Privacy Breaches, are available at http://www.privcom.gc.ca/media/nr-c/2007/nr-c_070801_guidelines_e.pdf and the Privacy Breach Checklist is available at http://www.privcom.gc.ca/media/nr-c/2007/nr-c_070801_checklist_e.pdf.

**UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION**

_____)
In the Matter of)
)
CARDSYSTEMS SOLUTIONS, INC.,)
a corporation.) **DOCKET NO. C-**
 _____)

COMPLAINT

The Federal Trade Commission, having reason to believe that CardSystems Solutions, Inc. (“respondent”) has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent CardSystems Solutions, Inc. is a Delaware corporation with its principal office or place of business at 6390 East Broadway, Tucson, Arizona 85710.
2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.

VIOLATIONS OF THE FEDERAL TRADE COMMISSION ACT

3. Respondent provides merchants with products and services used to obtain authorization for credit and debit card purchases (“card purchases”) from the banks that issued the cards (“issuing banks”). Last year, respondent provided authorization processing for card purchases totaling at least \$15 billion for approximately 119,000 merchants. In connection with these activities, respondent uses the Internet and a web application program (“web application”) to provide information to client merchants about authorizations that have been performed for them, and to provide information to prospective merchants about the services offered.
4. To obtain approval for a card purchase, merchants typically use respondent’s services to: collect information from the card’s magnetic stripe, including, but not limited to, customer name, card number and expiration date, a security code used to verify electronically that the card is genuine, and certain other information (collectively, “personal information”); format the information into an authorization request; and transmit the request to respondent’s authorization processing computer network. From

there, respondent transmits the request to a computer network operated by or for a bank association (such as Visa or MasterCard) or another entity (such as American Express), which transmits it to the issuing bank. The issuing bank receives the request, approves or declines the purchase, and transmits its response to the merchant over the same computer networks used to process the request. The response includes the personal information that was included in the authorization request the issuing bank received.

5. Since 1998, respondent has stored authorization responses for up to thirty (30) days in one or more databases on its computer network. Each day, these databases contain as many as several million authorization responses.
6. Respondent has engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information stored on its computer network. Among other things, respondent: (1) created unnecessary risks to the information by storing it in a vulnerable format for up to 30 days; (2) did not adequately assess the vulnerability of its web application and computer network to commonly known or reasonably foreseeable attacks, including but not limited to "Structured Query Language" (or "SQL") injection attacks; (3) did not implement simple, low-cost, and readily available defenses to such attacks; (4) failed to use strong passwords to prevent a hacker from gaining control over computers on its computer network and access to personal information stored on the network; (5) did not use readily available security measures to limit access between computers on its network and between such computers and the Internet; and (6) failed to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations.
7. In September 2004, a hacker exploited the failures set forth in Paragraph 6 by using an SQL injection attack on respondent's web application and website to install common hacking programs on computers on respondent's computer network. The programs were set up to collect and transmit magnetic stripe data stored on the network to computers located outside the network every four days, beginning in November 2004. As a result, the hacker obtained unauthorized access to magnetic stripe data for tens of millions of credit and debit cards.
8. In early 2005, issuing banks began discovering several million dollars in fraudulent credit and debit card purchases that had been made with counterfeit cards. The counterfeit cards contained complete and accurate magnetic stripe data, including the security code used to verify that a card is genuine, and thus appeared genuine in the authorization process. The magnetic stripe data matched the information respondent had stored on its computer network. In response, issuing banks cancelled and re-issued thousands of credit and debit cards. Consumers holding these cards were unable to use them to access their credit and bank accounts until they received replacement cards.

9. As set forth in Paragraphs 6, 7, and 8, respondent's failure to employ reasonable and appropriate security measures to protect personal information it stored caused or is likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.
10. The acts and practices of respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this ___ day of _____, 2006, has issued this complaint against respondent.

By the Commission

Donald S. Clark
Secretary

other available data that identifies an individual consumer; or (h) any other information from or about an individual consumer that is combined with (a) through (g) above.

2. Unless otherwise specified, "respondent" shall mean BJ's Wholesale Club, Inc. and its successors and assigns, officers, agents, representatives, and employees.

3. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

- A. the designation of an employee or employees to coordinate and be accountable for the information security program.
- B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.
- C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.
- D. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to respondent's operations or business

arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

II.

IT IS FURTHER ORDERED that respondent obtain an assessment and report (an "Assessment") from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession, within one hundred and eighty (180) days after service of the order, and biennially thereafter for twenty (20) years after service of the order that:

- A. sets forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
- B. explains how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers;
- C. explains how the safeguards that have been implemented meet or exceed the protections required by Paragraph I of this order; and
- D. certifies that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and, for biennial reports, has so operated throughout the reporting period.

Each Assessment shall be prepared by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondent shall provide the first Assessment, as well as all: plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relied upon to prepare such Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

III.

IT IS FURTHER ORDERED that respondent shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each document relating to compliance, including but not limited to:

- A. for a period of five (5) years: any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and
- B. for a period of three (3) years after the date of preparation of each biennial Assessment required under Paragraph II of this order: all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relating to respondent's compliance with Paragraphs I and II of this order for the compliance period covered by such biennial Assessment.

IV.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having managerial responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

V.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. *Provided, however,* that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Paragraph shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VI.

IT IS FURTHER ORDERED that respondent shall, within one hundred and eighty (180) days after service of this order, and at such other times as the Commission may require, file with the Commission an initial report, in writing, setting forth in detail the manner and form in which it has complied with this order.

VII.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however,* that the filing of such a complaint will not affect the duration of:

- A. any Paragraph in this order that terminates in less than twenty (20) years;
- B. this order's application to any respondent that is not named as a defendant in such complaint; and
- C. this order if such complaint is filed after the order has terminated pursuant to this Paragraph.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Paragraph as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

Signed this seventeenth day of May, 2005

BJ's WHOLESALE CLUB, INC.

By: _____
BJ's WHOLESALE CLUB, INC.

DAVID MEDINE
JAMES W. PRENDERGAST
Wilmer Cutler Pickering Hale and Dorr LLP
Counsel for respondent BJ's Wholesale Club, Inc.

FEDERAL TRADE COMMISSION

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

By: _____
ALAIN SHEER
Counsel for the Federal Trade Commission

_____)	
In the Matter of)	FILE NO. 0523148
)	
CARDSYSTEMS SOLUTIONS, INC.,)	AGREEMENT CONTAINING
a corporation, and)	CONSENT ORDER
)	
SOLIDUS NETWORKS, INC.)	
D/B/A PAY BY TOUCH SOLUTIONS,)	
a corporation.)	
_____)	

APPROVED:

JOEL WINSTON
Associate Director
Division of Financial Practices

LYDIA B. PARNES
Director
Bureau of Consumer Protection

The Federal Trade Commission has conducted an investigation of certain acts and practices of CardSystems Solutions, Inc., a Delaware corporation ("proposed respondent"). During the investigation, Solidus Networks, Inc., doing business as Pay By Touch Solutions, acquired the assets of CardSystems Solutions, Inc. CardSystems Solutions, Inc. and Solidus Networks, Inc., having been represented by counsel, are willing to enter into an agreement containing a consent order resolving the allegations contained in the attached draft complaint. Therefore,

IT IS HEREBY AGREED by and between CardSystems Solutions, Inc., by its duly authorized officers, Solidus Networks, Inc., by its duly authorized officers, and counsel for the Federal Trade Commission that:

1. Proposed respondent CardSystems Solutions, Inc. is a Delaware corporation with its principal office or place of business at 6390 East Broadway, Tucson, Arizona 85710.
2. Solidus Networks, Inc, doing business as Pay By Touch Solutions, is a Delaware corporation with its principal office or place of business at 101 2nd St Ste 1500, San Francisco, California 94105.
3. Proposed respondent admits all the jurisdictional facts set forth in the draft complaint.
4. Proposed respondent and Solidus Networks, Inc. waive:
 - A. any further procedural steps;

B. the requirement that the Commission's decision contain a statement of findings of fact and conclusions of law; and

C. all rights to seek judicial review or otherwise to challenge or contest the validity of the order entered pursuant to this agreement.

5. Solidus Networks, Inc. admits it is CardSystems' successor for the purposes of the order.

6. This agreement shall not become part of the public record of the proceeding unless and until it is accepted by the Commission. If this agreement is accepted by the Commission, it, together with the draft complaint, will be placed on the public record for a period of thirty (30) days and information about it publicly released. The Commission thereafter may either withdraw its acceptance of this agreement and so notify proposed respondent and Solidus Networks, Inc., in which event it will take such action as it may consider appropriate, or issue and serve its complaint (in such form as the circumstances may require) and decision in disposition of the proceeding.

7. This agreement is for settlement purposes only and does not constitute an admission by proposed respondent or Solidus Networks, Inc. that the law has been violated as alleged in the draft complaint, or that the facts as alleged in the draft complaint, other than the jurisdictional facts, are true.

8. This agreement contemplates that, if it is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to the provisions of Section 2.34 of the Commission's Rules, the Commission may, without further notice to proposed respondent and Solidus Networks, Inc., (1) issue its complaint corresponding in form and substance with the attached draft complaint and its decision containing the following order in disposition of the proceeding, and (2) make information about it public. When so entered, the order shall have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other orders. The order shall become final upon service. Delivery of the complaint and the decision and order to proposed respondent's address and Solidus Networks, Inc.'s address as stated in this agreement by any means specified in Section 4.4(a) of the Commission's Rules shall constitute service. Proposed respondent and Solidus Networks, Inc. waive any right they may have to any other manner of service. The complaint may be used in construing the terms of the order. No agreement, understanding, representation, or interpretation not contained in the order or in the agreement may be used to vary or contradict the terms of the order.

9. Proposed respondent and Solidus Networks, Inc. have read the draft complaint and consent order. They understand that they may be liable for civil penalties in the amount provided by law and other appropriate relief for each violation of the order after it becomes final.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. "Personal information" shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (d) a telephone number; (e) a Social Security number; (f) credit or debit card information, including card number, expiration date, and data stored on a card's magnetic stripe; (g) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; or (h) any other information from or about an individual consumer that is combined with (a) through (g) above.

2. Unless otherwise specified, "respondent" shall mean CardSystems Solutions, Inc. and its successors and assigns, including Solidus Networks, Inc., officers, agents, representatives, and employees.

3. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program.

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information,

and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.

D. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

II.

IT IS FURTHER ORDERED that, in connection with its compliance with Paragraph I of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
- B. explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers;
- C. explain how the safeguards that have been implemented meet or exceed the protections required by Paragraph I of this order; and
- D. certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondent shall provide the initial Assessment, as well as all: plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relied upon to prepare such Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

III.

IT IS FURTHER ORDERED that respondent shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each document relating to compliance, including but not limited to:

- A. for a period of five (5) years: any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and
- B. for a period of three (3) years after the date of preparation of each biennial Assessment required under Paragraph II of this order: all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relating to respondent's compliance with Paragraphs I and II of this order for the compliance period covered by such biennial Assessment.

IV.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having managerial responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

V.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. *Provided, however,* that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Paragraph shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Dated: October 28, 2005

CARDSYSTEMS SOLUTIONS, INC.

By: _____
CARDSYSTEMS SOLUTIONS, INC.

W. STEPHEN CANNON
Constantine Cannon
Counsel for respondent CardSystems Solutions, Inc.

VI.

IT IS FURTHER ORDERED that respondent shall, within one hundred and eighty (180) days after service of this order, and at such other times as the Commission may require, file with the Commission an initial report, in writing, setting forth in detail the manner and form in which it has complied with this order.

VII.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however,* that the filing of such a complaint will not affect the duration of:

- A. any Paragraph in this order that terminates in less than twenty (20) years;
- B. this order's application to any respondent that is not named as a defendant in such complaint; and
- C. this order if such complaint is filed after the order has terminated pursuant to this Paragraph.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Paragraph as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

ORIGINAL

SOLIDUS NETWORKS, INC. D/B/A/ PAY BY TOUCH SOLUTIONS

Dated: _____

By: _____
SOLIDUS NETWORKS, INC. D/B/A PAY BY TOUCH SOLUTIONS

CHRISTINE VARNEY
Hogan and Hartson LLP
Counsel for Solidus Networks, Inc.

FEDERAL TRADE COMMISSION

Dated: _____

By: _____
ALAIN SHEER
LARA KAUFMANN
MOLLY CRAWFORD

Counsel for the Federal Trade Commission

APPROVED:

JOEL WINSTON
Associate Director
Division of Financial Practices

LYDIA B. PARNES
Director
Bureau of Consumer Protection

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FILED IN CLERK'S OFFICE
U.S.D.C. - Atlanta

JAN 30 2006
LUTHER D. FORTNA, Clerk
By: _____
Deputy Clerk

UNITED STATES OF AMERICA,)
)
Plaintiff,)
)
v)
)
CHOICEPOINT INC., a corporation,)
)
Defendant.)

Civil Action No.

1 06 - CV - 0198

**COMPLAINT FOR CIVIL PENALTIES, PERMANENT INJUNCTION,
AND OTHER EQUITABLE RELIEF**

Plaintiff, the United States of America, acting upon notification and authorization to the Attorney General by the Federal Trade Commission ("FTC" or "Commission"), for its Complaint, alleges that.

1 Plaintiff brings this action under Sections 5(a), 13(b), and 16(a) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 45(a), 53(b), and 56(a); and Section 621(a) of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681s(a), to secure permanent injunction, consumer redress, disgorgement, and other equitable relief from Defendant for engaging in acts or practices violating Section 5(a) of the FTC Act, 15 U.S.C. § 45(a) and the FCRA, 15 U.S.C. §§ 1681-1681x; and to recover monetary civil penalties pursuant to Section 621(a)(2)(A) of the FCRA, 15 U.S.C. § 1681s(a)(2)(A).

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction over this matter under 28 U.S.C. §§ 1331, 1337(a), 1345, and 1355, and under 15 U.S.C. §§ 45(m)(1)(A), 53(b), 56(a), and 1691c(c)

3. Venue in the United States District Court for the Northern District of Georgia is proper under 15 U.S.C. § 53(b) and under 28 U.S.C. §§ 1391(b)-(c) and 1395(a).

DEFENDANT

4. Defendant ChoicePoint Inc., including for all purposes in this Complaint its subsidiaries and operating companies, ("ChoicePoint" or "Defendant"), is a Georgia corporation with its principal place of business at 1000 Alderman Drive, Alpharetta, Georgia 30005. In connection with the matters alleged herein, ChoicePoint has transacted business in this District.

5. At all times material to this Complaint, certain subsidiaries of ChoicePoint have collected and maintained personal identifying information about individuals, and have furnished that information to others for a fee. Among other lines of business, ChoicePoint sells to its subscribers consumer reports obtained from consumer reporting agencies and public record information obtained from a variety of sources.

6. Certain subsidiaries of ChoicePoint are "consumer reporting agencies" as that term is defined in Section 603(f) of the FCRA, 15 U.S.C. § 1681a(f)

COMMERCE

7. Defendant maintains, and at all times mentioned herein has maintained, a course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

DEFENDANT'S COURSE OF CONDUCT

8. ChoicePoint markets products and services to businesses, governments, and other entities that use the information contained in ChoicePoint's databases for, among other things, identification and credential verification purposes. ChoicePoint's products and services draw upon billions of records collected and maintained by ChoicePoint that contain the personal information of consumers, including names, Social Security numbers, dates of birth, bank and credit card account numbers, and credit histories, much of which is sensitive and not publicly available

9. ChoicePoint furnishes consumers' personal information, in various combinations and product lines, to businesses through a number of operating units. These operating units include, but are not limited to, ChoicePoint Public Records Group, WorkPlace Solutions, and Insurance Services. ChoicePoint Public Records Group provides public records data, such as bankruptcy and lien information, as well as identity verification products and services. These products contain the personal information of individual consumers, such as name, address, date of birth, and Social Security number. WorkPlace Solutions provides pre-employment and tenant screening products and services, including consumer reports. Insurance Services provides, among other things, products and services to the insurance industry for use in underwriting, including consumer reports.

10. ChoicePoint obtains consumer data from a broad assortment of sources, including, but not limited to, insurance claims data, public records (such as courthouses, recorders of deeds, and criminal dockets), motor vehicle records, and other consumer reporting agencies, including the three nationwide credit reporting agencies. ChoicePoint collects the information without making any contact with the consumers whose information it sells, and consumers cannot remove their information from ChoicePoint's databases.

11 A business obtains data from ChoicePoint by entering into an agreement and becoming a subscriber. In order to become a subscriber, an entity must submit an application that includes certain information and documentation to establish that the applicant is a legitimate business with a lawful purpose for purchasing consumer data. ChoicePoint then processes the application materials before approving or rejecting the account. ChoicePoint has over 50,000 subscribers, including insurance companies, landlords, banks, private investigators, debt collectors, and a variety of other businesses.

12. In February 2005, pursuant to a California state law requirement, ChoicePoint notified approximately 35,000 California consumers that it may have disclosed their personal information to persons who did not have a lawful purpose to obtain the information. Subsequently, ChoicePoint notified approximately 111,000 consumers outside of California that their information may have been compromised. More recently, it notified an additional 17,000 consumers, bringing the total to 163,000. In all cases, the information disclosed by ChoicePoint included unique identifying information that facilitates identity theft, such as dates of birth and Social Security numbers, as well as nearly 10,000 credit reports. At least 800 cases of identity theft arose out of these incidents.

13. The persons who obtained this consumer information submitted applications to ChoicePoint and were approved by the company to be subscribers authorized to purchase ChoicePoint products and services. The applications contained false credentials and other misrepresentations, which ChoicePoint failed to detect because it had not implemented reasonable procedures to verify or authenticate the identities and qualifications of prospective subscribers. Among other things, ChoicePoint failed to: utilize readily available business verification products, such as those that identify commercial mail drops; examine applications

and supporting documentation supplied by prospective new users, compare information supplied by prospective new users to information supplied by other applicants in order to identify suspect representations; conduct site visits; or utilize other reasonable methods to detect discrepancies, illogical information, suspicious patterns, factual anomalies, and other indicia of unreliability.

Examples of these failures include, but are not limited to, the following:

- a. ChoicePoint accepted as verification of certain application information (e.g., business address) documents that otherwise called into question the authenticity of the applicant's business or the reliability of information supplied by the applicant, such as a utility statement showing a delinquent account or a telephone statement showing billing at a residential, rather than a business, rate;
- b. ChoicePoint accepted for verification purposes documentation that included facially contradictory information, such as different business addresses on federal tax identification documents and utility statements, without conducting further inquiry to resolve the contradiction;
- c. ChoicePoint accepted other forms of facially contradictory or illogical application information, such as articles of incorporation that reflected that the business was suspended or inactive, and tax registration materials that showed that the business' registration was cancelled a few days prior to the date the application was submitted to ChoicePoint, without conducting further inquiry to resolve apparent anomalies;
- d. ChoicePoint accepted information inconsistent with the stated type of business of an applicant, such as an apartment number or commercial mail drop as the applicant's business address, or a cellular telephone number as the business' sole telephone number, without further inquiry to verify the authenticity of the applicant's business;

e. ChoicePoint approved, without further inquiry, the applications of subscribers notwithstanding the fact that the applicant left critical information, such as business license number, contact information, or applicant's last name, blank on the application;

f. ChoicePoint accepted applications transmitted by facsimile from public commercial locations, and accepted multiple applications for putatively separate businesses from the same facsimile numbers, without further inquiry to verify the authenticity of the applicant's business; and

g. ChoicePoint accepted and approved, without further inquiry, the applications of subscribers notwithstanding the fact that ChoicePoint's own internal reports on the applicant linked him or her to possible fraud associated with the Social Security number of another individual.

14. ChoicePoint also failed to monitor or otherwise identify unauthorized activity by subscribers, even after receiving subpoenas from law enforcement authorities between 2001 and 2005 alerting it to fraudulent accounts, and even when its own experiences with the subscriber should have raised doubts about the legitimacy of the subscriber's business. Examples of these failures include, but are not limited to, the following:

a. Furnishing to a purported apartment leasing subscriber a large number of consumer reports, over a relatively short period of time, that substantially exceeded the total number of rental units stated in the subscriber's application, without verifying that the applicant had a permissible purpose to obtain the reports;

b. Continuing to furnish consumer reports to a subscriber when the subscriber's telephone had been disconnected, the business address of the subscriber was found to be incorrect, the credit card number provided by the subscriber for payment to

ChoicePoint was in the name of an individual not associated with the subscriber's ChoicePoint account, the subscriber made multiple changes of address and/or telephone numbers over a short period of time, and the subscriber made payments to ChoicePoint solely by commercial money orders drawn on multiple issuers;

c. Continuing to furnish consumer reports to a subscriber when the subscriber's ChoicePoint account was repeatedly suspended for nonpayment; and

d. Continuing to furnish consumer reports to a subscriber when the documents submitted by that subscriber in the ChoicePoint application process were identified by ChoicePoint personnel as suspicious.

VIOLATIONS OF THE FCRA

COUNT I

15. Section 604 of the FCRA, 15 U.S.C. § 1681b, prohibits a consumer reporting agency from furnishing a consumer report except for specified "permissible purposes."

16. In numerous instances, ChoicePoint has furnished consumer reports to subscribers that did not have a permissible purpose to obtain a consumer report.

17. By and through the acts and practices described in Paragraph 16, ChoicePoint has violated Section 604(a) of the FCRA, 15 U.S.C. § 1681b(a)

COUNT II

18. Section 607(a) of the FCRA, 15 U.S.C. § 1681e(a), requires a consumer reporting agency to maintain reasonable procedures to limit the furnishing of consumer reports to the purposes listed under Section 604 of the FCRA, including making reasonable efforts to verify the identity of each new prospective user of consumer report information and the uses certified by each prospective user prior to furnishing such user a consumer report.

19. In numerous instances, ChoicePoint has failed to maintain reasonable procedures to limit the furnishing of consumer reports to the purposes listed under Section 604 of the FCRA, has failed to make reasonable efforts to verify the identity of prospective new users of consumer report information, and has failed to make reasonable efforts to verify the uses certified by each prospective user prior to furnishing such user a consumer report. For example, ChoicePoint has failed to examine or audit its subscribers to ensure that they were in fact using consumer report information for permissible purposes. In addition, ChoicePoint has failed to implement reasonable procedures, such as site visits, audits, or other verification, for users who typically have both permissible and impermissible purposes for using consumer reports (such as attorneys, insurance companies, private investigators, detective agencies, and protective service firms) to ensure that such users were using consumer report information for permissible purposes only.

20. Section 607(a) of the FCRA, 15 U.S.C. § 1681e(a), prohibits a consumer reporting agency from furnishing a consumer report to any person if it has reasonable grounds for believing that the consumer report will not be used for a permissible purpose.

21. In numerous instances, ChoicePoint has furnished consumer reports to subscribers under circumstances in which ChoicePoint had reasonable grounds for believing that the reports would not be used for a permissible purpose.

22. By and through the acts and practices described in Paragraphs 16, 19, and 21, ChoicePoint has violated Section 607(a) of the FCRA, 15 U.S.C. § 1681e(a).

23. Pursuant to Section 621(a)(1) of the FCRA, 15 U.S.C. § 1681s(a)(1), the alleged violations of the FCRA constitute unfair or deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

24. The acts and practices described in Paragraphs 16, 19, and 21 constitute a pattern or practice of knowing violations, as set forth in Section 621(a)(2)(A) of the FCRA, 15 U.S.C. § 1681s(a)(2)(A).

DEFENDANT'S VIOLATIONS OF SECTION 5 OF THE FTC ACT

COUNT III

25. As described in Paragraphs 12 through 14, ChoicePoint has not employed reasonable and appropriate measures to secure the personal information it collects for sale to its subscribers, including reasonable policies and procedures to (1) verify or authenticate the identities and qualifications of prospective subscribers; or (2) monitor or otherwise identify unauthorized subscriber activity

26. ChoicePoint's failure to employ reasonable and appropriate security measures to protect consumers' personal information has caused or is likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

COUNT IV

27. Since at least 1999, ChoicePoint has adopted various privacy principles, including but not limited to Exhibit A, which it has disseminated or caused to be disseminated on its websites at www.choicepoint.com and www.choicepoint.net, incorporated in its contracts with subscribers, and discussed in its Annual Reports filed with the Securities and Exchange Commission and distributed to shareholders and the public. These privacy principles contain the

following statement regarding the confidentiality and security of personal information collected, maintained, or furnished by ChoicePoint:

ChoicePoint uses administrative, technical, personnel, and physical safeguards to protect the confidentiality and security of personally identifiable consumer information in our possession. These safeguards are designed to ensure a level of security appropriate to the nature of the data being processed and the risks of confidentiality violations involved.

28. ChoicePoint maintains a website, www.choicetrust.com, which contains information directed at consumers. Through this website, ChoicePoint has disseminated or caused to be disseminated various notices about the FCRA, including but not necessarily limited to Exhibit B, containing the following statements:

Because ChoicePoint's ChoiceTrust understands its responsibility to treat consumers fairly and to protect their privacy, we have developed Fair Information Practices. These practices are derived from the Federal Fair Credit Reporting Act, but go beyond the requirements of that law. . . . ChoicePoint operated under its own Fair Information Practices even before passage of this Act, and continues to offer greater protection to the consumer than is required by the FCRA.

ChoicePoint allows access to your consumer reports only by those authorized under the FCRA. In addition, each ChoicePoint customer must verify that he/she has a 'permissible purpose' before receiving a consumer report.

29. ChoicePoint has disseminated or has caused to be disseminated a letter and Frequently Asked Questions (FAQ) to consumers who request a copy of their ChoicePoint public records file, including but not limited to Exhibit C, containing the following statement:

Every ChoicePoint customer must successfully complete a rigorous credentialing process. ChoicePoint does not distribute information

to the general public and monitors the use of its public record information to ensure appropriate use.

30. Through the means described in Paragraphs 27 through 29, Defendant has represented, expressly or by implication, that ChoicePoint has implemented reasonable and appropriate measures under the circumstances to maintain and protect the confidentiality and security of consumers' personal information, including a rigorous credentialing process for subscribers to prevent persons without a lawful purpose from obtaining access to consumers' personal information; and procedures to monitor subscribers' use of its public record information to ensure appropriate use.

31. In truth and in fact, ChoicePoint has not implemented reasonable and appropriate measures under the circumstances to maintain and protect the confidentiality and security of consumers' personal information, including a rigorous credentialing process for subscribers to prevent persons without a lawful purpose from obtaining access to consumers' personal information; or procedures to monitor subscribers' use of its public record information to ensure appropriate use. Therefore, the representations set forth in Paragraphs 27 through 29 were, and are, false or misleading in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

32. The acts and practices of ChoicePoint as alleged in Paragraphs 27 through 30 of this Complaint constitute deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THIS COURT'S POWER TO GRANT RELIEF

33. Each instance in which ChoicePoint has failed to comply with Sections 604 or 607 of the FCRA, 15 U.S.C. §§ 1681b, 1681e, constitutes a separate violation of the FCRA for the purpose of assessing monetary civil penalties.

34. Plaintiff seeks monetary civil penalties for every separate violation of the FCRA, which occurred each time ChoicePoint: (1) furnished a consumer report to a person who did not have a permissible purpose to obtain such a report; (2) furnished a consumer report under circumstances where ChoicePoint failed to make a reasonable effort to verify the identity of the prospective user and the uses certified by such prospective user prior to furnishing such user a consumer report, and (3) furnished a consumer report to any person when it had reasonable grounds for believing that the consumer report would not be used for a permissible purpose under the FCRA.

35. Section 621(a)(2)(A) of the FCRA, 15 U.S.C. § 1681s(a)(2)(A), authorizes the Court to award monetary civil penalties of not more than \$2,500 per violation.

36 Under Sections 5(m)(1)(A), and 13(b) of the FTC Act, 15 U.S.C. §§ 45(m)(1)(A), and 53(b), this Court is authorized to issue injunctive and such other and further equitable and ancillary relief as it may deem appropriate in the enforcement of the FCRA and the FTC Act, including consumer redress and disgorgement, to prevent and remedy any violations of any provision of law enforced by the Commission

PRAYER FOR INJUNCTIVE AND MONETARY RELIEF

WHEREFORE, Plaintiff requests that this Court, pursuant to 15 U.S.C. §§ 45(a)(1),

45(m)(1)(A), 53(b), 1681s, and 1691c, and pursuant to the Court's own equitable powers:

- (1) Enter judgment against Defendant and in favor of Plaintiff for each violation alleged in this Complaint;
- (2) Permanently enjoin Defendant from violating the FCRA and the FTC Act, as alleged herein;

- (3) Award Plaintiff monetary civil penalties from Defendant for each violation of the FCRA alleged in this Complaint;
- (4) Award all equitable relief that the Court finds necessary to redress injury to consumers resulting from Defendant's violations of the FCRA and the FTC Act, including, but not limited to, restitution, disgorgement, and other forms of redress;
- (5) Order Defendant to pay the costs of bringing this action; and
- (6) Award Plaintiff such additional equitable relief as the Court may deem just and proper

Dated Jan. 30, 2006

Of Counsel:

JOEL WINSTON
Associate Director for
Privacy and Identity Protection

JESSICA RICH
Assistant Director for
Privacy and Identity Protection

KATHRYN RATTÉ
MOLLY CRAWFORD
Attorneys
Division of Privacy and Identity Protection
Federal Trade Commission
Washington, D C 20580

FOR THE UNITED STATES OF AMERICA:

PETER D. KEISLER, JR
Assistant Attorney General
Civil Division
U.S. Department of Justice

DAVID E. NAHMIAS
United States Attorney
Northern District of Georgia

By: Amy L. Berne
AMY L. BERNE
Assistant United States Attorney
Georgia Bar No. 006670
Northern District of Georgia
600 United States Courthouse
75 Spring Street, S.W
Atlanta, Georgia 30303
Tel (404) 581-6261
Fax. (404) 581-6163

EUGENE M. THIROLF
Director
Office of Consumer Litigation

By: 

ALAN J. PHELPS
Trial Attorney
Office of Consumer Litigation
Civil Division
U.S. Department of Justice
Washington, D.C. 20530
Tel: (202) 307-6154
Fax: (202) 514-8742

Attorneys for Plaintiff
United States of America

Exhibit A

AGREEMENT FOR SERVICE - AGENTS/OTHERS

CHOICEPOINT PRIVACY PRINCIPLES
November 9, 1999

PREAMBLE

ChoicePoint is a leading provider of credentialing information about people and businesses that facilitates the establishment of business relationships for smarter decision-making. ChoicePoint is also a business leader in protecting and advocating consumer privacy.

ChoicePoint stands for responsible, effective and innovative use of personal information to help corporations, governments, and individuals make decisions that matter. This vision embraces using personal information to enhance security and will help people and businesses by bringing increased confidence to decision-makers. Just as importantly, this vision embraces developing consensual models to collaborate with consumers to deliver consumer services and to protect personal privacy. Increasingly, ChoicePoint will look to consumers as a source for the most accurate and timely information about the consumer and as partners in the appropriate use of consumer information to benefit both ChoicePoint's customers and the consumer.

Protecting privacy is always a ChoicePoint priority. Many of our products are already subject to important privacy protections provided by federal and state laws, such as the Fair Credit Reporting Act and its state law counterparts, or by self-regulatory principles, such as the Individual Reference Services Group ("IRSG") Principles. We are a founding member of the IRSG and we are a leader in the adoption and implementation of the IRSG Privacy Principles.

To underscore our fundamental commitment to privacy and our vision that good privacy is good business — for ChoicePoint, for our customers and for consumers — we have adopted the following Privacy Principles which are beyond those mandated by law or self-regulatory principles:

SCOPE

Our Privacy Principles apply to all personally identifiable information collected, maintained, or used in delivering information products and services by any ChoicePoint company or line of business as well as our agents and contractors. Of course, when information is subject to federal or state privacy law, we comply with that law and, in addition, adhere to our Privacy Principles so as to provide consumers with privacy privileges beyond those mandated by law.

1. RELEVANCE

ChoicePoint will collect, maintain, use, and disseminate personal information only to improve public safety, to reduce fraud, to improve risk management, to improve the quality of our customer services and products, or to help our customers drive down the cost of providing services and products.

ChoicePoint only collects, maintains, disseminates, and uses personally identifiable information for select products and services that serve socially useful purposes. Some ChoicePoint products, for example, help improve public safety by assisting law enforcement to track fugitives or by helping day care centers screen potential workers for criminal records. Other products we offer help insurance companies and other businesses to reduce fraud, allow patients to determine whether their doctors have had their licenses suspended or revoked, or assist employers in making employment decisions. Information products of this type provide critical benefits to consumers that justify the use of personally identifiable information provided that appropriate privacy standards are met. We understand the sensitive nature of the personally identifiable information contained in many of our information products and we rigorously protect this information and limit its use only to products that meet a stringent social utility test.

2. REPUTABLE SOURCES

We obtain personally identifiable information only from sources known to us to be reputable. These sources include courts, public record repositories, and consumer reporting agencies. In addition, we increasingly look for opportunities to obtain personally identifiable information on a cooperative, consensual basis from consumers and, further, look for opportunities to allow consumers to serve as a source of information about themselves through consumer review, correction, or amendment.

Reference number = <*REFNUM*>

Page 5

23 Agreement for Service -Agents/Others Form 145 (05/2001)
C.L.U.E. is a registered trademark, A.D.D. is a service mark, and ChoicePoint, the ChoicePoint logo, and NCF are trademarks of ChoicePoint Asset Company
©2001 ChoicePoint Asset Company. All rights reserved.

FO03983
CONFIDENTIAL

AGREEMENT FOR SERVICE - AGENTS/OTHERS

ChoicePoint places priority on the reliability of its information sources. ChoicePoint carefully reviews its source's information practices prior to using a source and ChoicePoint ceases to use a source if the source ceases to provide accurate, complete and timely information.

Oftentimes, the consumer is one of the best sources of information about the consumer. Where appropriate and possible, ChoicePoint will seek to develop consensual models to obtain consumer input and participation.

3. NOTICE/OPT-OUT

We inform consumers either directly or through notices in our brochures, on our web site, or through other public information and education opportunities, of the types of information we obtain about consumers, how and when that information is used, when it might be disclosed, and the steps we take to protect it. In addition, where appropriate, we allow consumers to opt-out of the dissemination of the personally identifiable information from our databases.

Increasingly, ChoicePoint is building direct or indirect contacts with consumers and, therefore, ChoicePoint's ability to offer opt-outs (where appropriate), provide notice or, at a minimum, educate the public about ChoicePoint and our products and services, is growing. While we work to give consumers greater control over their personal information, we do not permit consumers to opt-out of certain databases. For instance, ChoicePoint does not permit consumers to opt-out of our databases that are designed to combat fraud, as permitting consumers to opt-out of such a database would defeat the purpose of the database.

4. INTERNAL USES

We recognize that the personally identifiable information contained in many of our information products is sensitive. Therefore, we strictly limit access to personal information to those employees who need access in order to carry out their job responsibilities. All employees are prohibited from "browsing" through our files and databases. We train our employees in the application of our need-to-know standard. We periodically audit for compliance with this standard and we impose penalties for any failure to comply with this standard.

ChoicePoint has adopted a need to know standard for employee access to personally identifiable information. We emphasize this standard with a flat out prohibition against our employees, under any circumstances, browsing through our databases to obtain information on celebrities, friends, neighbors or others who may be of interest. We also train our employees in the application of our information use policies, we audit for compliance with these policies, and we will sanction employees who violate these policies.

5. DISCLOSURE TO CUSTOMERS AND OTHERS

ChoicePoint discloses personally identifiable information to customers and others only pursuant to consumer notices, consumer consent or when in compliance with law or legal process.

We provide personally identifiable information to customers to bring increased confidence to decision-makers. We insist that our customers use our personally identifiable information products and services in a manner consistent with our Privacy Principles.

For the vast majority of our business transactions, we obtain consent from the consumer directly or through our customers before we disclose information to third parties. However, in cases where consent is not practical, we provide notice through Web sites and education materials of the uses to which our information is put. In addition, however, we may be required by court order or subpoena to provide personally identifiable information without the consent of the consumer to whom it pertains.

6. ACCURACY

ChoicePoint strives to maintain the highest practicable data accuracy.

When we obtain information from public record repositories or other "official" sources, we seek to accurately capture and reflect the information obtained from these sources.

Reference number = <*REFNUM*>

Page 6

23 Agreement for Service -Agents/Others Form 145 (05/2001)
C.L.U.E. is a registered trademark, A.D.D. is a service mark, and ChoicePoint, the ChoicePoint logo, and NCF are trademarks of ChoicePoint Asset Company
©2001 ChoicePoint Asset Company. All rights reserved.

FO03984
CONFIDENTIAL

AGREEMENT FOR SERVICE - AGENTS/OTHERS

Information is the core of our business and providing accurate information is vital to our success. If a consumer notifies us that personally identifiable information is incorrect, we will either correct the information or direct the consumer to the source of the information for correction.

If, upon review, we believe that the existing information is correct, we will inform the consumer. If the consumer still disputes the accuracy of the information, we will note, if appropriate, the consumer dispute in our records.

7. CONSUMER ACCESS

ChoicePoint provides consumers with access to and copies of virtually all personally identifiable information we maintain on that consumer.

We believe that consumers should be able to find out what personally identifiable information we maintain about them. We believe that consumer access promotes accuracy and helps consumers to better understand the types of products and services that we provide and the benefits of those products.

There are some exceptions to this rule, including when providing access may have an adverse impact on the health or safety of the consumer, when access would violate the privacy of another individual or reveal the identity of a confidential source, when the information is processed by ChoicePoint but controlled by an outside party, when access is prohibited by law, or when the information requested is related to litigation involving ChoicePoint or its affiliates.

8. SECURITY

ChoicePoint uses administrative, technical, personnel and physical safeguards to protect the confidentiality and security of personally identifiable consumer information in our possession.

These safeguards are designed to ensure a level of security appropriate to the nature of the data being processed and the risks of confidentiality violations involved.

9. COMPLIANCE PROGRAM

ChoicePoint has implemented a comprehensive compliance program.

Compliance actions include:

- Training all ChoicePoint employees with access to personally identifiable information in the purpose and application of our Privacy Principles;
- Requiring employees with access to personally identifiable information to sign confidentiality agreements;
- Conducting background checks of employees hired for positions with access to personally identifiable information; and
- Holding employees accountable for violations of our privacy policies, with sanctions, including the possibility of termination of employment.

10. PRIVACY RESPONSIBILITY

To ensure that our privacy program receives high-level attention our Board of Directors has created a special committee to oversee the implementation and future development of our Privacy Principles.

In addition, a senior ChoicePoint official is responsible for implementing and overseeing the administration of our Privacy Principles on a day to day basis.

This official is responsible for:

- Working with a special committee of the Board of Directors on privacy issues;
- Working with our Human Resources Department to oversee our employee training program;
- Overseeing our consumer point of contact's resolution of privacy inquiries and complaints;

F003985
CONFIDENTIAL

Reference number = <*<REFNUM*>

Page 7

Agreement for Service - Agents/Others Form 145 (05/2001)
C.L.U.E. is a registered trademark, A.D.D. is a service mark, and ChoicePoint, the ChoicePoint logo, and NCF are trademarks of ChoicePoint Asset Company
©2001 ChoicePoint Asset Company All rights reserved.

23

AGREEMENT FOR SERVICE - AGENTS/OTHERS

- Working with our legal department to ensure our ongoing compliance with applicable privacy laws as well as our Privacy Principles;
- Overseeing our consumer education and outreach efforts; and
- Otherwise administering the implementation and enforcement of our Privacy Principles and other privacy matters.

11. COMPLIANCE ASSESSMENTS

ChoicePoint will conduct periodic compliance assessments of our internal practices to ensure that the Privacy Principles are being implemented effectively.

We take compliance with our policies seriously. We will assess our compliance with our Privacy Principles periodically to make sure that all of our business units are in compliance. Some assessments may also be conducted by outside parties.

12. INTERNET PRIVACY

ChoicePoint recognizes the importance of the privacy of information obtained over the Internet and applies its Privacy Principles to the online environment.

We have developed an online privacy policy reflecting our Privacy Principles and evolving standards for Internet privacy and we have placed these procedures, and our Privacy Principles, on our home page and the home pages of our business units. This privacy policy is easy to find, read, and understand. We give the consumer choice about the use of information collected about the consumer online. We also provide information about our data security measures, our data quality and access controls, and means to correct any inaccuracies in information collected about a consumer over the Internet.

We will maintain a "privacy seal" through a nationally recognized seal organization which applies the Online Privacy Alliance ("OPA") guidelines for Internet privacy and provides a dispute-resolution system for consumer complaints regarding online privacy.

13. GOOD STANDARDS/EDUCATION EFFORTS

ChoicePoint pledges that its business units will work actively to promote up-to-date and meaningful privacy standards for their industries.

We will participate actively in self-regulatory privacy initiatives as well as participating in the debate about developing privacy laws and regulations. We will also engage in consumer education efforts to promote privacy awareness.

14. CONSUMER POINT OF CONTACT AND DISPUTE RESOLUTION

ChoicePoint provides consumers with a point of contact to respond to consumer questions about our Privacy Principles and to assist consumers in exercising their options under our Privacy Principles.

With over 3,500 employees across the country, we know that finding the right employee to talk to is important for consumers.

Therefore, we provide consumers with a point of contact through a toll-free number and email. This point of contact will:

- Be available to answer consumer questions regarding our privacy policies and procedures;
- Direct the consumer to a point of contact in the relevant business unit;
- Address complaints from consumers regarding possible violations of our Privacy Principles; and
- Assist consumers in exercising their rights of opt-out, access, or correction under our Privacy Principles.

In the unlikely event that a disagreement with the consumer persists, we are committed to developing easy to use, consumer friendly procedures to resolve any dispute.

Reference number = <*<REFNUM*>

Page 8

Agreement for Service - Agents/Others Form 145 (05/2001)
C.L.U.E. is a registered trademark, A.D.D. is a service mark, and ChoicePoint, the ChoicePoint logo, and NCF are trademarks of ChoicePoint Asset Company
©2001 ChoicePoint Asset Company All rights reserved.

23

F003986
CONFIDENTIAL

Your FCRA Rights

Page 1 of 3

Click on the following state if you reside in CA, CT, MA, MD, NH, NJ, TX, VT, WA

Your FCRA Rights

Because ChoicePoint's ChoiceTrust understands its responsibility to treat consumers fairly and to protect their privacy, we have developed Fair Information Practices. These practices are derived from the Federal Fair Credit Reporting Act, but go beyond the requirements of that law. With your assistance, our Fair Information Practices can help you protect your privacy and achieve the fairest possible business dealings with insurance companies.

ChoicePoint operated under its own Fair Information Practices even before passage of this Act, and continues to offer greater protection to the consumer than is required by the FCRA.

What is the Fair Credit Reporting Act (FCRA)?

The Federal Fair Credit Reporting Act (FCRA) promotes accuracy, fairness and privacy of information in the files of every consumer-reporting agency (CRA). You can find the complete text of the FCRA 15 U.S.C. 1681 et seq., at www.ftc.gov.

Summary of Your Rights under the FCRA The Federal Fair Credit Reporting Act (FCRA) is designed to promote accuracy, fairness, and privacy of information in the files of every consumer reporting agency (CRA). Most CRAs are credit bureaus that gather and sell information about you – such as if you pay your bills on time or have filed bankruptcy – to creditors, employers, landlords, and other businesses. You can find the complete text of the FCRA, 15 U.S.C. 1681-1681u, at the Federal Trade Commission's web site (<http://www.ftc.gov>). The FCRA gives you specific rights, as outlined below. You may have additional rights under state law. You may contact a state or local consumer protection agency or a state attorney general to learn those rights.

- **You must be told if information in your file has been used against you.** Anyone who uses information from a CRA to take action against you – such as denying an application for credit, insurance, or employment – must tell you, and give you the name, address, and phone number of the CRA that provided the consumer report.
- **You can find out what is in your file.** At your request, a CRA must give you the information in your file, and a list of everyone who has requested it recently. There is no charge for the report if a person has taken action against you because of information supplied by the CRA, if you request the report within 60 days of receiving notice of the action. You also are entitled to one free report every twelve months upon request if you certify that (1) you are unemployed and plan to seek employment within 60 days, (2) you are on welfare, or (3) your report is inaccurate due to fraud. Otherwise, a CRA may charge you up to eight dollars.
- **You can dispute inaccurate information with the CRA.** If you tell a CRA that your consumer report contains inaccurate information, the CRA must investigate the items (usually within 30 days) by presenting to its information source all relevant evidence you submit, unless your dispute is frivolous. The source must review your evidence and report its findings to the CRA. (The source also must advise national CRAs – to which it has provided the data – of any error.) The CRA must give you a written report of the investigation, and a copy of your report if the investigation results in any change. If the CRA's investigation does not resolve the dispute, you may add a brief statement to your file. The CRA must normally include a summary of your statement in future reports. If an item is deleted or a dispute statement is filed, you may ask that anyone who has recently received your report be notified of the change.
- **Inaccurate information must be corrected or deleted.** A CRA must remove or correct inaccurate or unverified information from its files, usually within 30 days after you dispute it. However, the CRA is

http://www.choicepoint.com/xsl/faq/fcra/fcra_consumer.htm

9/6/2005

Exhibit B

not required to remove accurate data from your file unless it is outdated (as described below) or cannot be verified. If your dispute results in any change to your report, the CRA cannot reinsert into your file a disputed item unless the information source verifies its accuracy and completeness. In addition, the CRA must give you a written notice telling you it has reinserted the item. The notice must include the name, address and phone number of the information source.

- **You can dispute inaccurate items with the source of the information.** If you tell anyone – such as a creditor who reports to a CRA – that you dispute an item, they may not then report the information to a CRA without including a notice of your dispute. In addition, once you've notified the source of the error in writing, it may not continue to report the information if it is, in fact, an error.
- **Outdated information may not be reported.** In most cases, a CRA may not report negative information that is more than seven years old, ten years for bankruptcies.
- **Access to your file is limited.** A CRA may provide information about you only to people with a need recognized by the FCRA – usually to consider an application with a creditor, insurer, employer, landlord, or other business.
- **Your consent is required for reports that are provided to employers, or reports that contain medical information.** A CRA may not give out information about you to your employer, or prospective employer, without your written consent. A CRA may not report medical information about you to creditors, insurers, or employers without your permission.
- **You may choose to exclude your name from CRA lists for unsolicited credit and insurance offers.** Creditors and insurers may use file information as the basis for sending you unsolicited offers of credit or insurance. Such offers must include a toll-free phone number for you to call if you want your name and address removed from future lists. If you call, you must be kept off the lists for two years. If you request, complete, and return the CRA form provided for this purpose, you must be taken off the lists indefinitely.
- **You may seek damages from violators.** If a CRA, a user or (in some cases) a provider of CRA data, violates the FCRA, you may sue them in state or federal court.

The FCRA gives several different federal agencies authority to enforce the FCRA	
FOR QUESTIONS OR CONCERNS REGARDING:	PLEASE CONTACT:
CRA's, creditors and others not listed below	Federal Trade Commission Consumer Response Center - FCRA Washington, DC 20580 202-326-3761
National banks, federal branches/agencies of foreign banks (word "National" or initials "N A" appear in or after bank's name)	Office of the Comptroller of the Currency Compliance Management, Mail Stop 6-6 Washington, DC 20219 800-613-6743
Federal Reserve System member banks (except national banks, and federal branches/agencies of foreign banks)	Federal Reserve Board Division of Consumer & Community Affairs Washington, DC 20551 202-452-3693
Savings associations and	Office of Thrift Supervision

federally chartered savings banks (word "Federal" or initials "F S B" appear in federal institution's name)	Consumer Programs Washington, DC 20552 800-642-6929
Federal credit unions (words "Federal Credit Union" appear in institution's name)	National Credit Union Administration 1775 Duke Street Alexandria, VA 22314 703-518-6360
State-chartered banks that are not members of the Federal Reserve System	Federal Deposit Insurance Corporation Division of Compliance & Consumer Affairs Washington, DC 20429 800-934-FDIC
Air, surface, or rail common carriers regulated by former Civil Aeronautics Board or Interstate Commerce Commission	Department of Transportation Office of Financial Management Washington, DC 20590 202-366-1306
Activities subject to the Packers and Stockyards Act, 1921	Department of Agriculture Office of Deputy Administrator - GIPSA Washington, DC 20250 202-720-7051

To whom does ChoicePoint provide my Consumer Report?

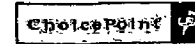
ChoicePoint allows access to your consumer reports only by those authorized under the FCRA. In addition, each ChoicePoint customer must verify that it has a "permissible purpose" before receiving a consumer report. When you sign an insurance application, you give the insurance company permissible purpose to order information reports related to your credit, driving history, and claims history.

Which products available through this site are Consumer Reports?

The claims, credit and driving record reports are considered consumer reports

[close window](#)

Exhibit C



ChoicePoint
Office of Privacy Compliance
1000 Alderman Drive, MD 71-K
Alpharetta, GA 30005

Dear Customer:

Thank you for ordering Your Personal Public Records Search from ChoicePoint. ChoicePoint is committed to the responsible use of information to help create a safer, more secure society while ensuring the protection of personal privacy. We are pleased to provide you with this report to help you better understand the information available through companies like ours and the positive power this information can have.

The following describes what is included in your custom search:

- Your Personal Public Records Search Results are based on the search we conducted through federal, state and local government agencies upon your recent request.
- Your Personal Non-Financial Credit Bureau Data Results Includes identity information obtained from the three national credit bureaus. This information is sometimes called credit header data and includes name, address and social security number. It does NOT include credit information or any financial data.
- Your Personal Publicly Available Records Search Results include information from published telephone directories. Please note that this information does not include unlisted numbers and addresses.

Please keep in mind the following important points when reviewing your results. Each record section has a detailed description about the source of the record. If you need more information, we have included a Q&A product sheet. Please review this information carefully. It's an easy way to get quick answers.

Results that you believe are inaccurate.

There are situations when a record may appear for someone else for a variety of reasons. Some records may appear because another person has lived at the same address and shares the same last name. There are also situations where the information has been recorded incorrectly by a reporting company or agency, or there may be fraudulent activity. If you believe that any information contained in this report is inaccurate, review the Q&A product sheet provided in this package for quick answers. If you still have concerns, you can request an inquiry package from us at:

ChoicePoint
Office of Privacy Compliance
1000 Alderman Drive, MD 71-K
Alpharetta, GA 30005

Or contact us by e-mail at: choicetrust_solutions@malco.custhelp.com

Sensitive Items in your report.

Some sensitive items in your report may be blocked with Xs. These Xs are used to protect your privacy and that of others that may be listed in the report.

- Social security numbers: (SSN) The last four digits of any SSNs of individuals who have been associated with you are substituted with Xs.
- Dates of birth: The specific date of birth is substituted with Xs.

This report provides you with valuable information about your public records. Thank you for your interest in ChoicePoint.

Thank you,

ChoicePoint Public Records Group
Consumer Disclosure Department

© 2004 ChoicePoint Asset Company. All rights reserved.

F000617
CONFIDENTIAL

76

ChoicePoint



Questions & Answers Product Sheet

General Questions**1. Who is ChoicePoint® ?**

ChoicePoint is one of the nation's leading providers of identification and credential verification services for making smarter decisions in a world challenged by increased risks.

ChoicePoint is also a trusted source of decision-making information that helps reduce fraud and mitigate risk.

Through the identification, retrieval, storage, analysis and delivery of data, ChoicePoint serves the informational needs of businesses of all sizes, as well as federal, state and local government agencies. ChoicePoint complies with federal, state, government agency laws and regulations regarding privacy.

2. What are Public Records?

Public records are records generated by various government entities including:

- Courts
- Licensing boards
- Secretaries of State
- Local government offices

Examples of public record information:

- County assessor records provide mailing and property addresses for real property owners across the United States.
- Secretary of State information locates corporations and limited partnerships, principal officers and registered agents throughout the United States.
- Professional licensing indexes identify addresses for individuals and businesses licensed in more than 40 professions.
- Bankruptcies, liens and judgments display addresses of individuals and businesses with derogatory financial histories.
- Uniform Commercial Code indexes provide identifying information on individuals and businesses with secured financing.

3. What are publicly available records?

Publicly available records are obtained from commonly used, non-governmental sources that are in the public domain. For example, this type of information is often gathered from published telephone directories. Please note, these records are based on historical data and do not include unlisted phone numbers and addresses.

F000618
CONFIDENTIAL

ChoicePoint



Questions & Answers Product Sheet

4. What are our information sources for Your Personal Public Records Search report?

Public records sources include:

- Property tax assessors offices – property ownership
- Deed recorders offices – deed transfers
- Federal Aviation Administration – aircraft and pilot licenses
- Secretaries of State – UCC filings, business affiliations, officer of a business, trademarks, service marks
- Federal bankruptcy courts – bankruptcies
- County civil courts – liens and judgments
- State licensing boards – professional licenses
- Federal Communications Commission – marine radio licenses
- Drug Enforcement Administration – DEA controlled substance licenses
- Bureau of Alcohol Tobacco and Firearms – federal firearms and explosives licenses
- Department of Defense – Active U.S. military personnel records
- Securities and Exchange Commission – significant shareholder records

Publicly available sources include:

- Telephone directory listings

Non-public information sources include:

- Social Security Administration
- Credit bureaus

5. Who uses ChoicePoint's public records data?

ChoicePoint only serves government agencies and legitimate businesses that have a permissible purpose to use public record data. Every ChoicePoint customer must successfully complete a rigorous credentialing process. ChoicePoint does not distribute information to the general public and monitors the use of its public record information to ensure appropriate use. ChoicePoint customers use public record information to combat fraud, find missing people, fight crime and minimize risk associated with business decisions.

6. Who has access to my information?

ChoicePoint's public records are restricted to professionals who must qualify for the service. Our subscribers include legal, professional and insurance industry investigators, and federal, state and local law enforcement agencies.

F000619
CONFIDENTIAL



Questions & Answers Product Sheet

7. Do you have FBI files?

No. ChoicePoint does not have access to FBI files.

8. How do I contact the credit bureaus?

There are three major credit bureaus in the United States (Experian, Equifax and TransUnion). You may contact them directly to obtain a copy of your credit report or inquire about changes and/or errors in your reported information. Toll-free telephone numbers for the three credit bureaus are shown below:

Experian 888-397-3742
Equifax 800-685-1111
TransUnion 800-888-4213

9. What can I do if I believe I have been a victim of Identity Theft?

There are a number of resources available to help you if you are a victim of identity theft. If you believe you are a victim, contact the fraud departments of the three major credit bureaus to obtain a copy of your credit report and to place a fraud alert on your credit file. The fraud alert requests creditors to contact you before opening any new accounts or making any changes to your existing accounts. Contact numbers for Equifax, Experian and TransUnion are:

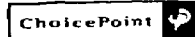
Equifax 800-685-1111
Experian 888-397-3742
TransUnion 800-888-4213

Please note, you do not have to be a victim of identity theft to place a fraud alert on your credit reports. This is a step many people take as a preventive measure to protect their identity. Remember, if you place a fraud alert on your credit file, it may delay any application for credit that you may submit in the future.

If you have confirmed that you have been a victim of identity fraud, here are some additional steps to take:

Contact your local and state authorities to determine whether they pursue identity theft cases. Even if your local police department will not pursue the case, file a police report. Get a copy of the report to submit to your creditors and others that may require proof of the crime.

Close the accounts that you believe have been tampered with or opened fraudulently. To dispute a new, unauthorized account, use the ID Theft Affidavit, available through the Federal Trade Commission. Go to www.ftc.gov or request one by calling 202-326-2222. You can also use the Broderbund Identity Theft Software, which includes all of the forms needed to address identity theft. (www.broderbund.com)



Questions & Answers Product Sheet

Some additional Web sites you may find useful are:

www.usdoj.gov/criminal/fraud/dtheft.html

www.consumer.gov/dtheft/

www.privacyrights.org/ftrc-quiz1.htm


Questions & Answers Product Sheet
Specific Questions about Your Personal Public Records Search Report
1. Why are other names listed with my social security number? When should I be concerned?

Multiple names can appear with your social security number for a number of reasons including:

- When applying for credit in the past, you may have used other names such as a nickname or maiden name, or you might be known by your middle name instead of your first name.
- Jointly filed public records
- Joint credit accounts (current and historical)
- Individuals with the same name (Jr., Sr.)
- There also might have been misspellings of your name
- There may be fraudulent activities associated with your name and social security number (see below).

IMPORTANT: Please pay special attention to the sections related to other individuals associated with your social security number. These sections, which are sourced from the three national credit bureaus, may show instances where your social security number has become associated with another individual's name. This typically happens through an input error; however, it can be a tip that a fraudulent activity may have occurred. Therefore, if another individual is associated with your social security number and you do not understand the reason, we urge you to obtain a credit report from the three national credit bureaus: Equifax, Experian and TransUnion.

Toll-free telephone numbers for the three credit bureaus are shown below:

Equifax 800-885-1111
 Experian 888-397-3742
 TransUnion 800-888-4213


*If you believe you are a victim of identity theft, please see general question #9: "What can I do if I believe I have been a victim of Identity Theft?"

2. Why is my report showing information that is old?

ChoicePoint does not exclude information in the search just because it is historical. ChoicePoint has information that is both current and historical in order to provide the most thorough data available.

3. Why is my report showing addresses at which I never lived?

The addresses that appear on your report are provided by the three major credit bureaus. Addresses that do not belong to you may appear because family members or former family members may have co-applied for credit or may have shared an address with you.


Questions & Answers Product Sheet
4. The report says I have a corporation, but I don't. Why?

Corporation records are returned two different ways in your report:

- 1) Business affiliations derived from Secretary of State corporation records will be listed when the last name and an address in your address history match those on a corporate record.
- 2) Possible officer of a business search results may be returned based on a name-only match.

Because limited information is used to match these records, information that does not pertain to you may be listed in order to provide all possible records.

5. Why are there typographical errors and mistakes in my report?

ChoicePoint provides a service by gathering and consolidating records on behalf of federal, state and local government agencies across the nation. Since ChoicePoint does not create the public record information in its possession, ChoicePoint does not have the right or ability to change or correct it.

6. Why don't you have my current address?

ChoicePoint provides the most up-to-date information available. As information is received from the three major credit bureaus, your report will be updated. If you have not updated your address with companies that report information to the credit bureaus, it may not appear.

7. Why do I have other social security numbers listed for my name?

Other social security numbers, names, dates of birth or addresses may be found when a search is run using your supplied social security number. These records are obtained from credit bureaus. Frequently other individuals are linked with social security numbers for several reasons including: jointly filed public records, joint credit accounts (current and historical), typographical errors, individuals with the same name (Jr., Sr.) and fraud. If you believe you are a victim of identity fraud, please see general question #9: "What can I do if I believe I have been a victim of Identity Theft?"

8. Why is my father's (or son's) information on my report?

Our report matches the name you supplied to our public records data on file. We do not make any distinction between "Juniors" and "Seniors" when matching names and this may be why you see fathers and sons listed.

ChoicePoint



Questions & Answers Product Sheet

9. Why don't you show the home I purchased under your property records?

Our property records are matched based on a name and exact match on the address including ZIP code. The information is retrieved from the county tax assessor's office on an annual basis, it may be that we were unable to produce an exact match on the address supplied or we have not yet received the annual update to our information.

10. What is a UCC?

The Universal Commercial Code (UCC) regulates secured transactions in which an individual or a business has secured the loan with some sort of collateral. UCC filings are derived from the applicable Secretary of State. The UCC filing records in your report match your last name and an address listed in your address history.

11. Why don't you show the UCC paid off (terminated)?

UCC updates are obtained from the Secretary of State in all 50 states at various intervals throughout the year. If we do not yet show the UCC paid off, our information may not yet be updated for this particular state.

12. Why is my professional license not listed?

Professional licenses are obtained from various state licensing boards at various intervals throughout the year. If we do not show your professional license, our information may not yet be updated. Depending on the state, we may or may not have professional license information for your profession.

13. What do the dates mean next to my addresses reported?

When reporting address information from a credit bureau, we pass along to you all dates noted on the addresses reported from the credit bureaus. This date is an internal indicator to the credit bureau and not ChoicePoint.

14. Why do you report old information when it's been corrected at the credit bureaus?

ChoicePoint does not exclude information in the search just because it is historical information. ChoicePoint has information that is both current and historical in order to provide the most thorough data available.

ChoicePoint



Questions & Answers Product Sheet

15. Why is my property appraised amount incorrect?

Property information is obtained from the county tax assessor's office. Each county reports on an annual basis. If you have specific questions about your property in the report, you may want to contact the county tax assessor for that property.

16. Can you get my court records?

No. In your personalized public records report only immediate information is made available. Typically, researchers must physically visit a courthouse to retrieve court records.

17. Will the report include criminal records?

No. Please visit the Self-Check Criminal product on www.ChoiceTrust.com.

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

_____)	
UNITED STATES OF AMERICA,)	
)	
)	
Plaintiff,)	Civil Action No.
)	
v.)	
)	
CHOICEPOINT INC., a corporation,)	
)	
Defendant.)	
_____)	

**STIPULATED FINAL JUDGMENT AND ORDER FOR CIVIL PENALTIES,
PERMANENT INJUNCTION, AND OTHER EQUITABLE RELIEF**

Plaintiff, the United States of America, acting upon notification and authorization to the Attorney General by the Federal Trade Commission (“FTC” or “Commission”), is concurrently filing its Complaint, which alleges that Defendant ChoicePoint Inc. has engaged in violations of the Fair Credit Reporting Act (“FCRA”), 15 U.S.C. §§ 1681-1681x, and in unfair or deceptive acts or practices in violation of Section 5 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45(a). The parties have agreed to the entry of this Stipulated Final Judgment and Order for Civil Penalties, Permanent Injunction, and Other Equitable Relief (“Order”) to resolve all matters in dispute in this action without trial or adjudication of any issue of law or fact herein and without Defendant admitting the truth of, or liability for, any of the matters alleged in the Complaint. Defendant has waived service of the Summons and Complaint.

THEREFORE, IT IS HEREBY ORDERED, ADJUDGED, AND DECREED as follows:

FINDINGS

1. This Court has jurisdiction over the subject matter of this case and over Defendant ChoicePoint Inc.
2. Venue in this district is proper under 28 U.S.C. § 1391(b) and (c), and 15 U.S.C. § 53(b).
3. The acts and practices of Defendant are in or affecting commerce, as “commerce” is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.
4. The Complaint states claims upon which relief may be granted against Defendant under Sections 5(a)(1), 13(b), 16(a), and 19 of the FTC Act, 15 U.S.C. §§ 45(a)(1), 53(b), 56(a), and 57b; and under Section 621(a) of the FCRA, 15 U.S.C. § 1681s(a).
5. Defendant makes no admissions to, and denies, the allegations in the Complaint, other than the jurisdictional facts.
6. Defendant waives: (a) all rights to seek appellate review or otherwise challenge or contest the validity of this Order; (b) any claim Defendant may have against the Commission, its employees, representatives, or agents that relate to the matter stated herein; (c) all claims under the Equal Access to Justice Act, 28 U.S.C. § 2412, as amended by Pub. L. 104-121, 110 Stat. 847, 863-64 (1996); and (d) any rights to attorneys’ fees that may arise under said provision of law.
7. Entry of this Order is in the public interest.

DEFINITIONS

For purposes of this Order, the following definitions shall apply:

1. "Fair Credit Reporting Act" or "FCRA" refers to 15 U.S.C. §§ 1681-1681x, as amended.

2. The terms "person," "consumer," "consumer report," and "consumer reporting agency" mean as defined in Sections 603(b), (c), (d), and (f), respectively, of the FCRA, 15 U.S.C. §§ 1681a(b), 1681a(c), 1681a(d), and 1681a(f).

3. "Permissible purpose" means any of the purposes listed in Section 604 of the FCRA, 15 U.S.C. § 1681b, for which a consumer reporting agency may lawfully furnish a consumer report.

4. "Subscriber" means any person or entity, excluding consumers, that enters into an agreement with Defendant pursuant to which that person or entity may request or obtain a consumer report or other personal information from Defendant.

5. "Mixed-use subscriber" means a subscriber that in the ordinary course of business typically has both permissible and impermissible purposes for ordering consumer reports.

6. "Personal information" means individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name or first initial and last name; (b) a home or other physical address, which includes at least street name and name of city or town; (c) an email address; (d) a telephone number; (e) a Social Security number; (f) credit and/or debit card information, including credit and/or debit card number with expiration date; (g) date of birth; (h) a driver's license number; or (i) any other information from or about an individual consumer that is combined with (a) through (h) above.

7. "Signing" or "signed" means either a handwritten signature (including those subsequently transmitted by facsimile, .pdf files, or other digital or electronic means) or an

"electronic signature" as that term is defined in the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7006(5).

8. Unless otherwise specified, "Defendant" means ChoicePoint Inc., its subsidiaries and operating companies, and their successors and assigns, officers, agents, representatives, and employees.

9. "Commerce" means as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

ORDER

I. CIVIL PENALTY

IT IS ORDERED that Defendant shall pay to Plaintiff, pursuant to Section 621(a) of the FCRA, 15 U.S.C. § 1681s(a), and Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A), a civil penalty in the amount of ten million dollars (\$10,000,000.00).

Defendant shall make the payment required by Paragraph I within seven (7) business days of the date of service of this Order by electronic fund transfer in accordance with instructions provided by the Office of Consumer Litigation, Civil Division, U.S. Department of Justice, Washington, D.C. 20530, for appropriate disposition.

In the event of any default in payment, which default continues for ten days beyond the due date of payment, the entire unpaid penalty, together with interest, as computed pursuant to 28 U.S.C. § 1961 from the date of default to the date of payment, shall immediately become due and payable.

II. PROHIBITED BUSINESS ACTIVITIES

IT IS FURTHER ORDERED that Defendant and all other persons or entities within the

scope of Fed. R. Civ. P. 65, whether acting directly or through any sole proprietorship, partnership, limited liability company, corporation, subsidiary, branch, division, or other entity, who receive actual notice of this Order by personal service or otherwise, are hereby permanently restrained and enjoined from:

A. Violating Section 604 of the FCRA, 15 U.S.C. § 1681b, by furnishing a consumer report to any person who does not have a permissible purpose to receive a consumer report.

B. Failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to subscribers that have permissible purposes to receive them under Section 604 of the FCRA, 15 U.S.C. § 1681b, as required by Section 607(a) of the FCRA, 15 U.S.C. § 1681e(a). Such procedures shall include, but not necessarily be limited to:

1. With respect to prospective subscribers, before furnishing a consumer report to any such subscriber; with respect to current subscribers, within one hundred eighty (180) days after the date of service of this Order; and with respect to subscribers of companies acquired by Defendant after the date of service of this Order, within ninety (90) days after the closing of the acquisition transaction for acquired companies with five thousand (5000) or fewer subscribers and within one hundred eighty (180) days after the closing of the acquisition transaction for acquired companies with more than five thousand (5000) subscribers:

- (a) Obtaining from each subscriber a written certification, either in paper or electronic form, stating the nature of the subscriber's business and all purposes for which the subscriber plans to obtain

consumer reports from Defendant. Each certification under this provision: (1) must be dated and signed; (2) must bear the printed or typed name of the person signing it; and (3) must state that the person signing it has direct knowledge of the facts certified; *provided, however*, that for current subscribers, the certification may, in lieu of stating that the person signing it has direct knowledge of the facts certified, attest to the truth of the matters certified and the authority of the person to sign on behalf of the subscriber.

- (b) Determining, based on the information in the subscriber's certification under subparagraph (a) above, and any other factors of which Defendant is aware or, under the circumstances, should reasonably ascertain, that each subscriber has a permissible purpose under Section 604 of the FCRA for the types of reports the subscriber plans to obtain, or, where the subscriber is a reseller of consumer reports, that the subscriber complies with Section 607(e)(2) of the FCRA.
- (c) As to subscribers that are businesses, verifying (1) the business identity of the subscriber; and (2) that the subscriber is a legitimate business engaged in the business certified and has a permissible purpose for obtaining consumer reports. Defendant shall conduct an on-site visual inspection of the business premises of each

subscriber, or, in the case of a subscriber with multiple locations, the headquarters location of the subscriber, *provided, however*, that

(i) for a prospective subscriber, Defendant does not need to conduct a site visit if Defendant independently verifies that at the time of application:

- (1) the applicant is a publicly held company under the regulatory authority of the United States Securities and Exchange Commission;
- (2) the applicant is subject to the regulatory authority of any agency listed in Section 621(b) of the FCRA, 15 U.S.C. § 1681s(b);
- (3) the applicant is an insurance agent sponsored by at least one insurance company that has been a subscriber of Defendant for at least one (1) year and has contractually agreed to assume financial responsibility for payment of the sponsored agent's acquisition of consumer reports from Defendant;
- (4) the applicant has been approved by the Internal Revenue Service as a tax-exempt organization pursuant to Section 501(c)(3) of the Internal Revenue Code, 26 U.S.C. § 501(c)(3), and as a subscriber will not receive from Defendant, unless

first provided to Defendant by the subscriber, any of the following information about consumers:

untruncated Social Security numbers; untruncated dates of birth; untruncated drivers' license numbers; or untruncated credit card, debit card, bank account, or other financial account numbers;

(5) the applicant has been certified by the Small Business Administration for participation in an SBA-administered program, such as the Section 8(a) Business Development program and the Small Disadvantaged Business Program, 13 C.F.R. part 124, or the Historically Underutilized Business ("HUBZone") program, 13 C.F.R. parts 121, 125, and 126; or

(6) the applicant has been certified by the Department of Transportation for participation in the Department of Transportation's Disadvantaged Business Enterprise Program, 49 C.F.R. part 26.

(ii) for a current subscriber, Defendant does not need to conduct a site visit if:

(1) Defendant has independently verified that at least one of the elements set out in (c)(i) above is

present with respect to that subscriber; or

(2) Defendant conducted a site visit within the one-year period immediately prior to the date of service of this Order that confirmed the legitimacy of the business, and the subscriber has not subsequently changed its address.

(iii) Defendant does not need to conduct a site visit for subscribers that are Federal or State agencies or departments that obtain consumer reports solely under Section 608 of the FCRA, 15 U.S.C. § 1681f, or that certify a permissible purpose solely under Sections 604(a)(3)(B), 604(a)(3)(D), 604(a)(4), 604(a)(5), 626, or 627, 15 U.S.C. §§ 1681b(a)(3)(B), (a)(3)(D), (a)(4), (a)(5); 1681u, or 1681v.

(d) Informing each subscriber in writing, either in paper or electronic form, that the FCRA imposes criminal penalties against anyone who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses, including a fine, up to two years in prison, or both, pursuant to Section 619 of the FCRA, 15 U.S.C. § 1681q, *provided* that the recitation of penalties shall be adjusted for any change in applicable law pursuant to Section 619 of the FCRA, 15 U.S.C. § 1681q.

- 9 -

(e) Providing to each subscriber to whom Defendant furnishes consumer reports a written copy of the "Notice to Users of Consumer Reports: Obligations of Users Under the FCRA," 16 C.F.R. Pt. 601 Appendix C, as required by Section 607(d) of the FCRA, 15 U.S.C. § 1681e(d), *provided, however*, that Defendant may furnish an electronic copy of this notice if a subscriber obtains consumer reports from Defendant in electronic form.

2. Beginning within thirty (30) days of the date of service of this Order, with respect to both current and prospective subscribers, or, with respect to subscribers of companies acquired by Defendant after the date of service of this Order, within sixty (60) days after the closing of the acquisition transaction:

(a) Each time any subscriber certifies a permissible purpose under Section 604(a)(3) of the FCRA, requiring the subscriber to identify and certify the specific subsection of Section 604(a)(3) (either by section or description, such as "insurance underwriting") that provides the permissible purpose to obtain the report.

(b) Requiring each mixed-use subscriber that certifies a permissible purpose under Section 604(a)(3)(A) of the FCRA to further identify and certify with specificity the intended use under that subsection each time it requests a consumer report (e.g., an attorney subscriber who certifies a permissible purpose under Section 604(a)(3)(A)

- 10 -

would also specify that it is “collecting a debt”); *provided* that such certification may be made at log-on, rather than on a per consumer report basis, in cases where the subscriber orders consumer reports through an interactive electronic ordering system operated by Defendant, and the subscriber has contractually certified only one permissible purpose specified in Section 604(a)(3)(A) to obtain consumer reports.

- (c) Requiring, each time any subscriber certifies as its permissible purpose a “legitimate business need” pursuant to Section 604(a)(3)(F) of the FCRA, that the subscriber certify and identify with specificity that business need (e.g., “in connection with applications for apartment rentals” or “applications to open checking accounts”). In those cases where a subscriber has permissible purposes that encompass more than one “legitimate business need” under Section 604(a)(3)(F), then individual certification and identification with specificity must be obtained by Defendant each time the subscriber requests a consumer report.
- (d) Ensuring that the following message, or one substantially identical to it, is displayed clearly and conspicuously on the subscriber’s screen each time a subscriber transmits a request electronically for a consumer report: “The federal Fair Credit Reporting Act imposes criminal penalties – including a fine, up to two years in prison, or

both – against anyone who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses, and other penalties for anyone who obtains such consumer information without a permissible purpose,”

provided that the recitation of penalties shall be adjusted for any change in applicable law pursuant to Section 619 of the FCRA, 15 U.S.C. § 1681q.

- (e) Employing reasonable procedures to verify that subscribers obtaining consumer reports are, in fact, using the reports solely for permissible purposes. Such procedures may include, but are not limited to, periodic Defendant-initiated audits that rely, at least in part, upon consumer or other non-subscriber third-party documentation of permissible purposes; *provided* that Defendant is not required to obtain additional verification of the permissible purpose with respect to any consumer report for which Defendant has received and retained for purposes of demonstrating compliance with this subparagraph:
- (1) a copy of a court order or a federal grand jury subpoena ordering the release of such report;
 - (2) verified documentation signed by the consumer on whom the report was furnished expressly authorizing the release of such report;

(3) in the case of a report for which the purpose certified was the collection of a judgment, a copy of the court judgment;

(4) in the case of a report for which the purpose certified was the evaluation of an employee for promotion, reassignment, or retention, a copy of an official business record (e.g., a W-2 Form) clearly identifying the subscriber or the subscriber's principal as the employer of the consumer on whom the report was furnished; or

(5) verification that the subscriber is a Federal or State agency or department that obtains consumer reports solely under Section 608 of the FCRA, 15 U.S.C. § 1681f, or that certifies a permissible purpose solely under Sections 604(a)(3)(B), 604(a)(3)(D), 604(a)(4), 604(a)(5), 626, or 627 of the FCRA, 15 U.S.C. §§ 1681b(a)(3)(B), (a)(3)(D), (a)(4), (a)(5); 1681u, and 1681v.

(f) Desisting from furnishing consumer reports to any subscriber as to which:

(1) Defendant learns, through the procedures described in subparagraph (e), or otherwise, has obtained, after the date of service of this Order, a consumer report for any purpose other than a permissible purpose, unless: (i) that subscriber obtained such report through inadvertent error, *i.e.*, a mechanical, electronic, or clerical error that the subscriber demonstrates was unintentional

and occurred notwithstanding the maintenance of procedures reasonably designed to avoid such errors; or (ii) such consumer report was obtained through the actions of a person acting without subscriber authorization, such as by using such subscriber's user identification and password, and the subscriber demonstrates that it has implemented reasonable and appropriate procedures to prevent a similar action or error from recurring; or

(2) Defendant has reasonable grounds to believe will not use the report solely for permissible purposes.

III. INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that Defendant and all other persons or entities within the scope of Fed. R. Civ. P. 65, whether acting directly or through any sole proprietorship, partnership, limited liability company, corporation, subsidiary, branch, division, or other entity, who receive actual notice of this Order by personal service or otherwise, are hereby permanently restrained and enjoined from, no later than the date of service of this Order:

A. Failing to establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to Defendant's size and complexity, the nature and scope of Defendant's activities, and the sensitivity of the personal

information collected from or about consumers, including:

1. The designation of an employee or employees to coordinate and be accountable for the information security program.
2. The identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (a) employee training and management; (b) information systems, including network and software design, information processing, storage, transmission, and disposal; and (c) prevention, detection, and response to attacks, intrusions, or other systems failures.
3. The design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.
4. The evaluation and adjustment of Defendant's information security program in light of the results of the testing and monitoring required by subparagraph 3, any material changes to Defendant's operations or business arrangements, or any other circumstances that Defendant knows or has reason to know may have a material impact on the effectiveness of its information security program.

- 15 -

B. Misrepresenting in any manner, expressly or by implication, the manner or extent to which Defendant maintains and protects the privacy, confidentiality, or security of any personal information collected from or about consumers.

IV. BIENNIAL ASSESSMENT REQUIREMENTS

IT IS FURTHER ORDERED that Defendant shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional who uses procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the Order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the Order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific administrative, technical, and physical safeguards that Defendant has implemented and maintained during the reporting period to comply with Paragraph III of this Order;
- B. explain how such safeguards are appropriate to Defendant's size and complexity, the nature and scope of Defendant's activities, and the sensitivity of the personal information collected from or about consumers;
- C. explain how the safeguards that have been implemented meet or exceed the protections required by Paragraph III of this Order; and
- D. certify that Defendant's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal

- 16 -

information is protected and, for biennial reports, has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission.

Defendant shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) business days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by Defendant until three years after completion of the final Assessment and provided to the Associate Director of Enforcement upon request within ten (10) business days after Defendant receives such request.

V. CONSUMER REDRESS

IT IS FURTHER ORDERED that no later than ten (10) days after the date of service of this Order, Defendant shall pay to the Federal Trade Commission the sum of five million dollars (\$5,000,000.00) under the following terms and conditions:

A. The payment shall be made by wire transfer or certified or cashier's check made payable to the Federal Trade Commission. In the event of any default in payment, which default

continues for ten (10) days beyond the due date of payment, the amount due, together with interest, as computed pursuant to 28 U.S.C. § 1961 from the date of default to the date of payment, shall immediately become due and payable.

B. All funds paid pursuant to this Paragraph shall be deposited into a fund administered by the Commission or its agent to be used for equitable relief, including but not limited to consumer redress and any attendant expenses for the administration of any redress fund. Any consumer redress distributed by the Commission pursuant to this Part shall be accompanied by a statement that provision of such redress by the Commission does not constitute an admission by Defendant of wrongdoing. In the event that direct redress to consumers is wholly or partially impracticable or funds remain after redress is completed, the Commission may apply any remaining funds for such other equitable relief (including information remedies) as it determines to be reasonably related to Defendant's practices alleged in the Complaint. Any funds not applied by the Commission for equitable relief shall be deposited to the United States Treasury. Defendant shall have no right to challenge the Commission's choice of remedies under this Paragraph.

No portion of any payments under this Paragraph shall be deemed a payment of any fine, penalty, punitive assessment, or forfeiture.

VI. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring and investigating compliance with any provision of this Order,

A. Within thirty (30) days of receipt of written notice from a representative of the

Commission, Defendant shall submit additional written reports, sworn to under penalty of perjury; produce documents for inspection and copying; appear for deposition; and/or provide entry during normal business hours to any business location in Defendant's possession or direct or indirect control, to inspect the business operation.

B. In addition, the Commission is authorized to monitor compliance with this Order by all other lawful means, including but not limited to the following:

1. Obtaining discovery from any person, without further leave of Court, using the procedures prescribed by Fed. R. Civ. P. 30, 31, 33, 34, 36, and 45.
2. Posing as consumers and suppliers to Defendant, Defendant's employees, or any other entity managed or controlled in whole or in part by Defendant, without the necessity of identification or prior notice.

C. Defendant shall permit representatives of the Commission to interview any consultant, independent contractor, representative, agent, or employee who has agreed to such an interview, relating in any way to any conduct subject to this Order. The person interviewed may have counsel present.

Provided that nothing in this Order shall limit the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1, to obtain any documentary material, tangible things, testimony, or information relevant to unfair or deceptive acts or practices in or affecting commerce (within the meaning of 15 U.S.C. § 45(a)(1)).

VII. COMPLIANCE REPORTING BY DEFENDANT

IT IS FURTHER ORDERED that, in order that compliance with the provisions of this Order may be monitored:

A. For a period of twenty (20) years from the date of service of this Order, Defendant shall notify the Commission of any changes in corporate structure that may affect compliance obligations arising under this Order, including but not limited to a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor entity; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices that are subject to this Order; the filing of a bankruptcy petition; or a change in the corporate name or address, at least thirty (30) days prior to such change, *provided* that, with respect to any proposed change in the corporation about which Defendant learns less than thirty (30) days prior to the date such action is to take place, Defendant shall notify the Commission as soon as is practicable after obtaining such knowledge.

B. One hundred eighty (180) days after the date of service of this Order, Defendant shall provide a written report to the FTC, sworn to under penalty of perjury, setting forth in detail the manner and form in which it has complied and is complying with this Order. This report shall include, but not be limited to:

1. Any changes required to be reported pursuant to Paragraph VII.A.
2. A copy of each acknowledgment of receipt of this Order obtained pursuant to Paragraph IX.

C. For the purposes of this Order, Defendant shall, unless otherwise directed by the Commission's authorized representatives, mail all written notifications to the Commission to:

Associate Director, Division of Enforcement
Bureau of Consumer Protection

Federal Trade Commission
Washington, D.C. 20580

D. For purposes of the compliance reporting and monitoring required by this Order, the Commission is authorized to communicate directly with Defendant.

VIII. RECORD KEEPING

IT IS FURTHER ORDERED that:

A. For a period of six (6) years from the date of service of this Order, Defendant and its agents, employees, officers, corporations, successors, and assigns, and those persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise, are hereby restrained and enjoined from failing to create and retain the following records:

1. Subscriber files containing the names, addresses, telephone numbers, all certifications made by the subscriber pursuant to Section 607(a) of the FCRA and Paragraph II.B.1(a)-(b) of this Order, and all materials considered by Defendant in connection with its verification of the identity of the subscriber and verification of the certifications made under Section 607(a), as required by Section 607(a) of the FCRA and Paragraph II.B.1(c) of this Order.
2. Consumer complaints (whether received in written or electronic form, directly, indirectly or through any third party), and any responses to those complaints, whether in written or electronic form, that relate to Defendant's activities as alleged in the Complaint and Defendant's

compliance with the provisions of this Order.

3. Copies of all training materials that relate to Defendant's activities as alleged in the Complaint and Defendant's compliance with the provisions of this Order.
4. Copies of all subpoenas and other communications with law enforcement entities or personnel, whether in written or electronic form, if such documents bear in any respect on Defendant's collection, maintenance, or furnishing of consumer reports or other personal information of consumers.
5. All records and documents necessary to demonstrate full compliance with each provision of this Order, including but not limited to, copies of acknowledgments of receipt of this Order, required by Paragraph IX.B, and all reports submitted to the FTC pursuant to Paragraph VII.

B. For a period of three (3) years after the date of preparation of each biennial Assessment required under Paragraph IV of this Order: all plans, reports, studies, reviews, audits, audit trails, policies, training materials, work papers, and assessments, whether prepared by or on behalf of Defendant, relating to Defendant's compliance with Paragraph III of this Order for the compliance period covered by such biennial Assessment.

IX. DISTRIBUTION OF ORDER BY DEFENDANT

IT IS FURTHER ORDERED that, for a period of five (5) years from the date of service of this Order, Defendant shall deliver copies of this Order as directed below:

A. Defendant shall deliver a copy of this Order to all of its officers and directors, and to all managers who have responsibility directly or indirectly for any matters covered by this Order. Defendant also shall deliver an accurate summary of this Order to all of its employees who are engaged in conduct related to Defendant's compliance with Section 607(a) of the FCRA, including but not limited to those employees who verify the identity of prospective users of consumer reports, those employees who verify the uses certified to Defendant by prospective users of consumer reports, and those employees who monitor or audit the continued compliance by Defendant's subscribers with their certification of permissible purposes. Defendant also shall deliver an accurate summary of this Order to all of its employees who are engaged in conduct related to Defendant's activities that are the subject of Paragraphs III and IV of this Order, including but not limited to those employees designated as information security program coordinators. For current personnel, delivery shall occur within ten (10) business days of the date of service of this Order upon Defendant. For new personnel, delivery shall occur no later than when they assume their job responsibilities.

B. Defendant shall secure a signed and dated statement acknowledging receipt of this Order, within thirty (30) days of delivery to such persons, from each person receiving a copy of the Order pursuant to this Paragraph IX.

X. ACKNOWLEDGMENT OF RECEIPT OF ORDER BY DEFENDANT

IT IS FURTHER ORDERED that Defendant, within five (5) business days of service of this Order, shall submit to the Commission a truthful sworn statement acknowledging receipt of this Order, in the form shown on Attachment A.

XI. RETENTION OF JURISDICTION

IT IS FURTHER ORDERED that this Court shall retain jurisdiction of this matter for purposes of construction, modification, and enforcement of this Order.

XII. COSTS AND ATTORNEYS' FEES

IT IS FURTHER ORDERED that each party shall bear its own costs and attorneys' fees incurred in connection with this action.

XIII. NOTICE OF ENTRY OF ORDER

IT IS FURTHER ORDERED that entry in the docket of this Order by the Clerk of Court shall constitute notice to Defendant of the terms and conditions of this Order, and that Defendant waives all rights to contest in any future proceeding whether Defendant was properly served with this Order.

The parties hereby stipulate to the entry of the foregoing Order, which shall constitute a final Order in this action.

IT IS SO ORDERED:

Dated this _____ day of _____, 2006

UNITED STATES DISTRICT JUDGE

The parties, by their respective counsel, hereby consent to the terms and conditions of the Stipulated Order as set forth above and consent to the entry thereof. Defendant waives any rights that may arise under the Equal Access to Justice Act, 28 U.S.C. § 2412, as amended by Pub. L. 104-121, 110 Stat., 847, 863-64 (1996).

FOR THE UNITED STATES OF AMERICA:

PETER D. KEISLER, JR.
Assistant Attorney General
Civil Division
U.S. Department of Justice

DAVID E. NAHMIAS
United States Attorney
Northern District of Georgia

Dated: _____

By: _____

AMY L. BERNE
Assistant United States Attorney
Georgia Bar No. 006670
Northern District of Georgia
600 United States Courthouse
75 Spring Street, S.W.
Atlanta, Georgia 30303
Tel: (404) 581-6261
Fax: (404) 581-6163

Dated: _____

ALAN J. PHELPS
Trial Attorney
Office of Consumer Litigation
Civil Division
U.S. Department of Justice
Washington, D.C. 20530
Tel: (202) 307-6154
Fax: (202) 514-8742

FOR THE FEDERAL TRADE COMMISSION:

Joel C. Winston
Associate Director for Privacy and Identity Protection

Jessica Rich
Assistant Director for Privacy and Identity Protection

Kathryn D. Ratté
Attorney

Molly Crawford
Attorney
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission
Washington, D.C. 20580
(202) 326-3224

FOR THE DEFENDANT, ChoicePoint Inc.:

Doug Curling
President, ChoicePoint Inc.

Robert R. Belair
Karla J. Letsche
Kevin L. Coy
Oldaker, Biden & Belair, LLP
818 Connecticut Avenue, N.W.
Suite 1100
Washington, D.C. 20006
Attorneys for Defendant

ATTACHMENT A

Joel Jankowsky
Daniel Ferrel McInnis
Akin Gump Strauss Hauer & Feld LLP
1333 New Hampshire Avenue, N.W.
Washington, D.C. 20036
Attorney for Defendant

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA

UNITED STATES OF AMERICA,)	CV
Plaintiff,)	
v.)	AFFIDAVIT OF
CHOICEPOINT INC., a)	DEFENDANT
corporation,)	CHOICEPOINT INC.
Defendant.)	

[Name of Defendant's certifying official], being duly sworn, hereby states and affirms as follows:

1. My name is _____. My current residence address is _____ I am a citizen of the United States and am over the age of eighteen. I have personal knowledge of the facts set forth in this Affidavit.
2. I am an officer of Defendant ChoicePoint in *United States of America v. ChoicePoint Inc.* (United States District Court for the Northern District of Georgia).
3. On _____, I received a copy of the Stipulated Final Judgment and Order for Civil Penalties, Permanent Injunction, and Other Equitable Relief, which was signed by the Honorable _____ and entered by the Court on _____. A true and correct copy of the Order I received is appended to this Affidavit.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct. Executed on _____, 2006, at _____.

By:

State of _____, City of _____

Subscribed and sworn to before me
this _____ day of _____, 2006.

Notary Public

My Commission Expires:

**PREPARED STATEMENT OF THE
FEDERAL TRADE COMMISSION**

Before the

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

U.S. SENATE

on

DATA BREACHES AND IDENTITY THEFT

June 16, 2005

I. INTRODUCTION

Mr. Chairman, I am Deborah Platt Majoras, Chairman of the Federal Trade Commission.¹ My fellow Commissioners and I appreciate the opportunity to appear before you today as we work to ensure the safety and security of consumers' personal information.

As we have testified previously, advances in commerce, computing, and networking have transformed the role of consumer information. Modern consumer information systems can collect, assemble, and analyze information from disparate sources, and transmit it almost instantaneously. Among other things, this technology allows businesses to offer consumers a wider range of products, services, and payment options; greater access to credit; and faster transactions.

Efficient information systems – data that can be easily accessed, compiled, and transferred – also can lead to concerns about privacy and security. Recent events validate concerns about information systems' vulnerabilities to misuse, including identity theft.

II. BACKGROUND

One particular focus of concern has been “data brokers,” companies that specialize in the collection and distribution of consumer data. Data brokers epitomize the tension between the benefits of information flow and the risks of identity theft and other harms. Data brokers have emerged to meet the information needs of a broad spectrum of commercial and government users.² The data broker industry is large and complex and includes companies of all sizes. Some

¹ This written statement reflects the views of the Federal Trade Commission. Our oral statements and responses to any questions you may have represent the views of individual Commissioners and do not necessarily reflect the views of the Commission.

² For more information on how consumer data is collected, distributed, and used, see generally Government Accountability Office, *Private Sector Entities Routinely Obtain and use SSNs, and Laws Limit the Disclosure of this*

collect information from original sources, both public and private; others resell data collected by others; and many do both. Some provide information only to government agencies or large companies, while others sell information to smaller companies or the general public as well. The amount and scope of the information that they collect varies from company to company, and many offer a range of products tailored to different markets and uses. These uses include fraud prevention, debt collection, law enforcement, legal compliance, applicant authentication, market research, and almost any other function that requires the collection and aggregation of consumer data. Because these databases compile sensitive information, they are especially attractive targets for identity thieves.

Identity theft is a crime that harms both consumers and businesses. A 2003 FTC survey estimated that nearly 10 million consumers discovered that they were victims of some form of identity theft in the preceding 12 months, costing American businesses an estimated \$48 billion in losses, and costing consumers an additional \$5 billion in out-of-pocket losses.³ The survey looked at the two major categories of identity theft: (1) the misuse of existing accounts; and (2) the creation of new accounts in the victim's name. Not surprisingly, the survey showed a direct correlation between the type of identity theft and its cost to victims, in both the time and

Information (GAO-04-11) (2004); Government Accountability Office, *Social Security Numbers: Use is Widespread and Protections Vary, Testimony Before the House Subcommittee on Social Security, Committee on Ways and Means* (GAO-04-768T) (statement of Barbara D. Bovbjerg, June 15, 2004); Federal Trade Commission, *Individual Reference Services: A Report to Congress* (December 1997), available at <http://www.ftc.gov/os/1997/12/irs.pdf>. The Commission also has held two workshops on the collection and use of consumer information: “Information Flows, The Costs and Benefits to Consumers and Businesses of the Collection and Use of Consumer Information,” was held on June 18, 2003; and “The Information Marketplace: Merging and Exchanging Consumer Data,” was held on March 13, 2001. An agenda, participant biographies, and a transcript for these workshops are available at <http://www.ftc.gov/bcp/workshops/infoflows/030618agenda.html> and <http://www.ftc.gov/bcp/workshops/informktplace/index.html>, respectively.

³ Federal Trade Commission, *Identity Theft Survey Report* (Sept. 2003), available at <http://www.ftc.gov/os/2003/09/synovatereport.pdf>.

money spent resolving the problems. For example, although people who had new accounts opened in their names made up only one-third of the victims, they suffered two-thirds of the direct financial harm. The ID theft survey also found that victims of the two major categories of identity theft cumulatively spent almost 300 million hours – or an average of 30 hours per person – correcting their records and reclaiming their good names. Identity theft causes significant economic and emotional injury, and we take seriously the need to reduce it.

As detailed in our recent testimony on this subject,⁴ there are a variety of existing federal laws and regulations that address the security of, and access to, sensitive information that these companies maintain, depending on how that information was collected and how it is used. For example, the Fair Credit Reporting Act (“FCRA”)⁵ regulates credit bureaus, any entity or individual who uses credit reports, and the businesses that furnish information to credit bureaus.⁶ The FCRA requires that sensitive credit report information be used only for certain permitted purposes. The Gramm-Leach-Bliley Act (“GLBA”)⁷ prohibits financial institutions from disclosing consumer information to non-affiliated third parties without first allowing consumers

to opt out of the disclosure. GLBA also requires these businesses to implement appropriate safeguards to protect the security and integrity of their customer information.⁸

In addition, Section 5 of the Federal Trade Commission Act (“FTC Act”) prohibits “unfair or deceptive acts or practices in or affecting commerce.”⁹ Under the FTC Act, the Commission has broad jurisdiction to prohibit unfair or deceptive practices by a wide variety of entities and individuals operating in commerce. Prohibited practices include deceptive claims that companies make about privacy, including claims about the security they provide for consumer information.¹⁰ To date, the Commission has brought five cases against companies for deceptive security claims.¹¹ These actions alleged that the companies made explicit or implicit promises to take reasonable steps to protect sensitive consumer information, but because they allegedly failed to take such steps, their claims were deceptive. The consent orders settling these cases have required the companies to implement appropriate information security programs that generally conform to the standards that the Commission set forth in the GLBA Safeguards Rule.

In addition to deception, the FTC Act prohibits unfair practices. Practices are unfair if they cause or are likely to cause consumers substantial injury that is neither reasonably avoidable

⁴ See, e.g., Statement of the Federal Trade Commission Before the Subcommittee on Financial Institutions and Consumer Credit, Committee on Financial Services, U.S. House of Representatives, on Enhancing Data Security: The Regulators’ Perspective (May 18, 2005), available at <http://www.ftc.gov/opa/2005/05/databrokertest.htm>.

⁵ 15 U.S.C. §§ 1681-1681x.

⁶ Credit bureaus are also known as “consumer reporting agencies.”

⁷ 15 U.S.C. §§ 6801-09.

⁸ The FTC’s Safeguards Rule implements GLBA’s security requirements for entities under the FTC’s jurisdiction. See 16 C.F.R. pt. 314 (“GLBA Safeguards Rule”). The federal banking regulators also have issued comparable regulations for the entities under their jurisdiction.

⁹ 15 U.S.C. § 45(a).

¹⁰ Deceptive practices are defined as material representations or omissions that are likely to mislead consumers acting reasonably under the circumstances. *Cliffdale Associates, Inc.*, 103 F.T.C. 110 (1984).

¹¹ *Petco Animal Supplies, Inc.* (FTC Docket No. C-4133) (Mar. 4, 2005); *MTS Inc., d/b/a Tower Records/Books/Video* (FTC Docket No. C-4110) (May 28, 2004); *Guess?, Inc.* (FTC Docket No. C-4091) (July 30, 2003); *Microsoft Corp.* (FTC Docket No. C-4069) (Dec. 20, 2002); *Eli Lilly & Co.* (FTC Docket No. C-4047) (May 8, 2002). Documents related to these enforcement actions are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

by consumers nor offset by countervailing benefits to consumers or competition.¹² The Commission has used this authority to challenge a variety of injurious practices that threaten data security.¹³

As the Commission has testified previously, an actual breach of security is not a prerequisite for enforcement under Section 5; however, evidence of such a breach may indicate that the company's existing policies and procedures were not adequate.¹⁴ It is important to note, however, that there is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution.¹⁵

Despite the existence of these laws, recent security breaches have raised questions about whether data brokers and other companies that collect or maintain sensitive personal information are taking adequate steps to ensure that the information they possess does not fall into the wrong hands, as well as about what steps should be taken when such data is acquired by unauthorized individuals. Vigorous enforcement of existing laws and business education about the requirements of existing laws and the importance of good security can go a long way in addressing these concerns. Nonetheless, recent data breaches have prompted Congress to

¹² 15 U.S.C. § 45(n).

¹³ These include, for example, unauthorized charges in connection with "phishing," which are high-tech scams that use spam or pop-up messages to deceive consumers into disclosing credit card numbers, bank account information, Social Security numbers, passwords, or other sensitive information. See *FTC v. Hill*, Civ. No. H 03-5537 (filed S.D. Tex. Dec. 3, 2003), available at <http://www.ftc.gov/opa/2004/03/phishingilljoint.htm>; *FTC v. C.J.*, Civ. No. 03-CV-5275-GHK (RZX) (filed C.D. Cal. July 24, 2003), available at <http://www.ftc.gov/os/2003/07/phishingcomp.pdf>.

¹⁴ See Statement of the Federal Trade Commission Before the House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform (Apr. 21, 2004) at 5, available at <http://www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf>.

¹⁵ *Id.* at 4.

consider legislative proposals, and the Commission has been asked to comment on the need for new legal requirements.

III. INCREASING CONSUMER INFORMATION SECURITY

The Commission recommends that Congress consider whether companies that hold sensitive consumer data, for whatever purpose, should be required to take reasonable measures to ensure its safety. Such a requirement could extend the FTC's existing GLBA Safeguards Rule to companies that are not financial institutions.

Further, the Commission recommends that Congress consider requiring companies to notify consumers when the security of this information has been breached in a manner that creates a significant risk of identity theft.¹⁶ Whatever language is chosen should ensure that consumers receive notices when they are at risk of identity theft, but not require notices to consumers when they are not at risk. As discussed below, the goal of any notification requirement is to enable consumers to take steps to avoid the risk of identity theft. To be effective, any such requirement must provide businesses with adequate guidance as to when notices are required.

In addition, many have raised concerns about misuse of Social Security numbers. It is critical to remember that Social Security numbers are vital to current information flows in the granting and use of credit and the provision of financial services. In addition, private and public entities routinely have used Social Security numbers for many years to access their voluminous records. Ultimately, what is required is to distinguish between legitimate and illegitimate collection, uses, and transfers of Social Security numbers.

¹⁶ Commissioner Harbour is concerned about the use of the term "significant" to characterize the level of risk of identity theft that should trigger a notice to consumers.

Finally, law enforcement activity to protect data security is increasingly international in nature. Given the globalization of the marketplace, an increasing amount of U.S. consumer information may be accessed illegally by third parties outside the United States or located in offshore databases. Accordingly, the Commission needs new tools to investigate whether companies are complying with U.S. legal requirements to maintain the security of this information, and cross-border fraud legislation would give the Commission these tools. For that reason, the Commission recommends that Congress enact cross-border fraud legislation to overcome existing obstacles to information sharing and information gathering in cross-border investigations and law enforcement actions.¹⁷

For example, if the FTC and a foreign consumer protection agency are investigating a foreign business for conduct that violates both U.S. law and the foreign country's law, current law does not authorize the Commission to share investigative information with the foreign consumer protection agency, even if such sharing would further our own investigation. New cross-border fraud legislation could ease these restrictions, permit the sharing of appropriate investigative information with our foreign counterparts, and give us additional mechanisms to help protect the security of U.S. consumers' data whether it is located abroad or in the United States.

A. Require Procedures to Safeguard Sensitive Information

One important step to reduce the threat of identity theft is to increase the security of certain types of sensitive consumer information that could be used by identity thieves to misuse existing accounts or to open new accounts, such as Social Security numbers, driver's license numbers, and

¹⁷ The U.S. Senate passed cross-border fraud legislation last year by unanimous consent: S. 1234 ("International Consumer Protection Act").

account numbers in combination with required access codes or passwords.¹⁸ Currently, the Commission's Safeguards Rule under GLBA requires financial institutions to implement reasonable physical, technical, and procedural safeguards to protect customer information. Instead of mandating specific technical requirements that may not be appropriate for all entities and might quickly become obsolete, the Safeguards Rule requires companies to evaluate the nature and risks of their particular information systems and the sensitivity of the information they maintain, and to take appropriate steps to counter these threats. They also must periodically review their data security policies and procedures and update them as necessary. The Safeguards Rule provides a strong but flexible framework for companies to take responsibility for the security of information in their possession, and it reflects widely accepted principles of information security, similar to those contained in the Organization for Economic Cooperation and Development's Guidelines for the Security of Information Systems and Networks.¹⁹

Currently, the Safeguards Rule applies only to "customer information" collected by "financial institutions."²⁰ It does not cover many other entities that may also collect, maintain and transfer or sell sensitive consumer information. Although we believe that Section 5 already requires companies holding sensitive data to have in place procedures to secure it if the failure to

¹⁸ The FTC also would seek civil penalty authority for its enforcement of these provisions. A civil penalty is often the most appropriate remedy in cases where consumer redress is impracticable and where it is difficult to compute an ill-gotten gain that should be disgorged from a defendant.

¹⁹ FTC Commissioner Orson Swindle led the U.S. delegation to the OECD Committee that drafted the 2002 OECD Security Guidelines. See Organization for Economic Cooperation and Development, *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (July 25, 2002), available at http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html.

²⁰ Under GLBA, a "financial institution" is defined as an entity that engages in one or more of the specific activities listed in the Bank Holding Company Act and its implementing regulations. See 15 U.S.C. § 6809(3). These activities include extending credit, brokering loans, financial advising, and credit reporting.

do so is likely to cause substantial consumer injury, we believe Congress should consider whether new legislation incorporating the flexible standard of the Commission's Safeguards Rule is appropriate.

B. Notice When Sensitive Information Has Been Breached

Unfortunately, even if the best efforts to safeguard data are made, security breaches can still occur. The Commission believes that if a security breach creates a significant risk of identity theft or other related harm, affected consumers should be notified. Prompt notification to consumers in these cases can help them mitigate the damage caused by identity theft. Notified consumers can request that fraud alerts be placed in their credit files, obtain copies of their credit reports, scrutinize their monthly account statements, and take other steps to protect themselves.

The challenge is to require notices only when there is a likelihood of harm to consumers. There may be security breaches that pose little or no risk of harm, such as a stolen laptop that is quickly recovered before the thief has time to boot it up. Requiring a notice in this type of situation might create unnecessary consumer concern and confusion. Moreover, if notices are required in cases where there is no significant risk to consumers, notices may be more common than would be useful. As a result, consumers may become numb to them and fail to spot or act on those risks that truly are significant. In addition, notices can impose costs on consumers and on businesses, including businesses that were not responsible for the breach. For example, in response to a notice that the security of his or her information has been breached, a consumer may cancel credit cards, contact credit bureaus to place fraud alerts on his or her credit files, or obtain a new driver's license number. Each of these actions may be time-consuming for the consumer, and costly for the companies involved and ultimately for consumers generally.

Currently there are two basic approaches in place that are used to determine when notices should be triggered. The first is the bank regulatory agency standard.²¹ Under that standard, notice to the federal regulatory agency is required as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information. In addition, notice to consumers is required when, based on a reasonable investigation of an incident of unauthorized access to sensitive customer information, the financial institution determines that misuse of its information about a customer has occurred or is reasonably possible.²²

The second approach is found in the California notice statute.²³ Under that approach, all businesses are required to provide notices to their consumers when a defined set of sensitive data, in combination with information that can be used to identify the consumer, has been or is reasonably likely to have been acquired by an unauthorized person in a manner that "compromises the security, confidentiality, or integrity of personal information."²⁴

The California "unauthorized acquisition" approach to requiring consumer notice does not compel notice in every instance of improper access to a database. Instead, it allows businesses some flexibility to determine when a notice is necessary, while also providing a fairly objective standard against which compliance can be measured by the broad range of businesses subject to

²¹ See Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736-54 (Mar. 29, 2005).

²² Under the guidance, this determination can be made by the financial institution in consultation with its primary federal regulator.

²³ Cal. Civ. Code § 1798.82.

²⁴ *Id.* at § 1798.82(d).

the law. Under guidance issued by the California Office of Privacy Protection, a variety of factors can be considered in determining whether information has been “acquired,” such as (1) indications that protected data is in the physical possession and control of an unauthorized person (such as a lost or stolen computer or other device); (2) indications that protected data has been downloaded or copied; or (3) indications that protected data has been used by an unauthorized person, such as to open new accounts.²⁵ One issue that is not directly considered is what action to take in cases in which, prior to sending consumer notification, the business already has taken steps that remedy the risk. For example, one factor to consider in deciding whether to provide notice is whether the business already has canceled consumers’ credit card accounts and reissued account numbers to the affected consumers.

We have growing experience under both models to inform consideration of an appropriate national standard. Because formulating any standard will require balancing the need for a clear, enforceable standard with ensuring, to the extent possible, that notices go to consumers only where there is a risk of harm, we believe that if Congress decides to enact a notice provision, the best approach would be to authorize the FTC to conduct a rulemaking under general statutory standards. The rulemaking would set the criteria under which notice would be required for data breaches involving non-regulated industries. The rulemaking could address issues such as the circumstances under which notice is required, which could depend on the type of breach and risk of harm, and the appropriate form of notice. This approach would also allow the Commission to adjust the standard as it gains experience with its implementation.

²⁵ These factors are discussed in the California Office of Privacy Protection’s publication, *Recommended Practices on Notification of Security Breach Involving Personal Information*, at 11 (Oct. 10, 2003), available at <http://www.privacy.ca.gov/recommendations/secbreach.pdf>.

C. Social Security Numbers

Social Security numbers today are a vital instrument of interstate commerce. With 300 million American consumers, many of whom share the same name,²⁶ the unique 9-digit Social Security number is a key identification tool for business. As the Commission found in last year’s data matching study under FACTA, Social Security numbers also are one of the primary tools that credit bureaus use to ensure that the data furnished to them is placed in the right file and that they are providing a credit report on the right consumer.²⁷ Social Security numbers are used in locator databases to find lost beneficiaries, potential witnesses, and law violators, and to collect child support and other judgments. Social Security number databases are used to fight identity fraud – for example, they can confirm that a Social Security number belongs to a particular loan applicant and is not stolen.²⁸ Without the ability to use Social Security numbers as personal identifiers and fraud prevention tools, the granting of credit and the provision of other financial services would become riskier and more expensive and inconvenient for consumers.

While Social Security numbers have important legitimate uses, their unauthorized use can facilitate identity theft. Identity thieves use the Social Security number as a key to access the financial benefits available to their victims. Currently, there are various federal laws that place

²⁶ According to the Consumer Data Industry Association, 14 million Americans have one of ten last names, and 58 million men have one of ten first names.

²⁷ See Federal Trade Commission, *Report to Congress Under Sections 318 and 319 of the Fair and Accurate Credit Transactions Act of 2003* at 38-40 (Dec. 2004), available at <http://www.ftc.gov/reports/facta/041209factarpt.pdf>.

²⁸ The federal government also uses Social Security numbers as an identifier. For example, HHS uses it as the Medicare identification number, and the IRS uses it as the Taxpayer Identification Number. It also is used to administer the federal jury system, federal welfare and workmen’s compensation programs, and the military draft registration. See Social Security Administration, *Report to Congress on Options for Enhancing the Social Security Card* (Sept. 1997), available at www.ssa.gov/history/reports/ssnreporte2.html.

some restrictions on the disclosure of specific types of information under certain circumstances. The FCRA, for example, limits the provision of “consumer report” information to certain purposes, primarily those determining consumers’ eligibility for certain transactions, such as extending credit, employment, or insurance. GLBA requires that “financial institutions”²⁹ provide consumers an opportunity to opt out before disclosing their personal information to third parties, outside of specific exceptions, such as for fraud prevention or legal compliance.³⁰ Other statutes that limit information disclosure include the privacy rule under the Health Insurance Portability and Accountability Act of 1996,³¹ which applies to health care providers and other medical-related entities, and the Drivers Privacy Protection Act,³² which protects consumers from improper disclosures of driver’s license information by state motor vehicle departments.

While these laws provide important privacy protections within their respective sectors, they do not provide comprehensive protection for Social Security numbers.³³ For example, disclosure of a consumer’s name, address, and Social Security number may be restricted under GLBA when the source of the information is a financial institution,³⁴ but in many cases the same

²⁹ See *supra* n.20 (defining financial institution).

³⁰ GLBA protects some, but not all Social Security numbers held by financial institutions. It does not, for example, cover Social Security numbers in databases of Social Security numbers furnished by banks to credit bureaus under the Fair Credit Reporting Act (i.e., so-called “credit header” information) prior to the GLBA Privacy Rule’s July 2001 effective date.

³¹ 45 C.F.R. pts. 160 and 164 (implementing Sections 262 and 264 of the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191).

³² 18 U.S.C. §§ 2721-25.

³³ The Commission may, however, bring enforcement actions under Section 5 of the Federal Trade Commission Act against entities whose privacy or security practices are unfair or deceptive.

³⁴ See *supra* n.30 (discussing limitations of GLBA protection).

information can be purchased on the Internet from a non-financial institution. The problem of how to strengthen or expand existing protections in ways that would not interfere with the beneficial uses of Social Security numbers is challenging.

Although the Commission has extensive experience with identity theft and the consumer credit reporting system, restrictions on disclosure of Social Security numbers could have a broad impact on areas where the Commission does not have expertise. These areas include public health, criminal law enforcement, and anti-terrorism efforts. Moreover, efforts to restrict disclosure of Social Security numbers are complicated by the fact that among the primary sources of Social Security numbers are the public records on file with many courts and clerks in cities and counties across the nation. Regulation or restriction of Social Security numbers in public records thus poses substantial policy and practical concerns.

Ultimately, what is required is to distinguish between legitimate and illegitimate collection, uses, and transfers of Social Security numbers. The Commission would appreciate the opportunity to work with Congress to further evaluate the costs and benefits to consumers and the economy of regulating the collection, transfer, and use of Social Security numbers.

IV. CONCLUSION

New information systems have brought benefits to consumers and businesses alike. Never before has information been so portable, accessible, and flexible. Indeed, sensitive personal financial information has become the new currency of today’s high tech payment systems. But with these advances come new risks, and identity thieves and other bad actors have begun to take advantage of new technologies for their own purposes. As the recent focus on information security has demonstrated, Americans take their privacy seriously, and we must ensure that the

many benefits of the modern information age are not diminished by these threats to consumers' security. The Commission is committed to ensuring the continued security of consumers' personal information and looks forward to working with you to protect consumers.

052-3096

**UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION**

_____)
In the Matter of)
)
DSW Inc.,)
a corporation.) **DOCKET NO. C-**
_____)

COMPLAINT

The Federal Trade Commission, having reason to believe that DSW Inc. ("respondent") has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent DSW Inc. is an Ohio corporation with its principal office or place of business at 4150 East 5th Avenue, Columbus, Ohio 43219.
2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.
3. Respondent sells footwear for men and women at approximately 190 stores in 32 states. Consumers pay for their purchases with cash, credit cards, debit cards, and personal checks.
4. For credit card, debit card, and check purchases at its stores, respondent uses computer networks to request and obtain authorization for the purchase. To obtain card authorization, respondent collects information from consumers, including name, card number and expiration date, and certain other information. To obtain approval for payments by check, respondent collects the routing number, account number, check number, and the consumer's driver's license number and state (collectively, "personal information").
5. For a credit or debit card purchase, respondent typically collects the information from the magnetic stripe of the credit or debit card. The information collected from the magnetic stripe includes, among other things, a security code used to verify electronically that the card is genuine. This code is particularly sensitive because it can be used to create

counterfeit credit and debit cards that appear genuine in the authorization process. For purchases using a check, respondent typically collects information from the check using Magnetic Ink Character Recognition ("MICR") technology. In each case, respondent collects the information at the cash register and wirelessly transmits the information, formatted as an authorization request, to a computer network located in the store ("in-store computer network"). The authorization request is then transmitted to the appropriate bank or check processor, which sends a response back to respondent through the same networks. Until at least March 2005, respondent stored personal information used to obtain credit card, debit card, and check authorizations, including magnetic stripe data, on in-store and corporate computer networks.

6. Respondent operates wireless access points through which the cash registers connect to the in-store computer networks. Other wireless access points are used to transmit information about respondent's inventory from in-store scanners to the in-store computer networks.
7. Until at least March 2005, respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information collected at its stores. Among other things, respondent (1) created unnecessary risks to the information by storing it in multiple files when it no longer had a business need to keep the information; (2) did not use readily available security measures to limit access to its computer networks through wireless access points on the networks; (3) stored the information in unencrypted files that could be accessed easily by using a commonly known user ID and password; (4) did not limit sufficiently the ability of computers on one in-store network to connect to computers on other in-store and corporate networks; and (5) failed to employ sufficient measures to detect unauthorized access. As a result, a hacker could use the wireless access points on one in-store computer network to connect to, and access personal information on, the other in-store and corporate networks.
8. In March 2005, respondent issued a press release stating that credit card and other purchase information stored on its computer networks had been stolen. In April 2005, respondent issued another press release listing the locations of 108 stores that were affected by the breach, and stating that checking account and driver's license numbers also had been subject to the breach. In April 2005, respondent also began sending notification letters to customers for whom it had or obtained addresses.
9. The breach compromised a total of approximately 1,438,281 credit and debit cards (but not the personal identification numbers associated with the debit cards), along with 96,385 checking accounts and driver's license numbers. To date, there have been fraudulent charges on some of these accounts. Further, some customers whose checking account information was compromised were advised to close their accounts, thereby losing access to those accounts, and have incurred out-of-pocket expenses such as the cost of ordering new checks. Some of these checking account customers have contacted DSW requesting reimbursement for their out-of-pocket expenses, and DSW has provided

some amount of reimbursement to these customers.

10. As described in Paragraph 7 above, respondent's failure to employ reasonable and appropriate security measures to protect personal information and files caused or is likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was and is an unfair act or practice.
11. The acts and practices of respondent as alleged in this complaint constitute unfair acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C § 45(a).

THEREFORE, the Federal Trade Commission this ___ day of ____, 2006, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary

FILE NO. 052 3096

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

)	
In the Matter of)	DOCKET NO.
)	
DSW Inc.,)	AGREEMENT CONTAINING
a corporation.)	CONSENT ORDER
)	

The Federal Trade Commission has conducted an investigation of certain acts and practices of DSW Inc., an Ohio corporation (“proposed respondent”). Proposed respondent, having been represented by counsel, is willing to enter into an agreement containing a consent order resolving the allegations contained in the attached draft complaint. Therefore,

IT IS HEREBY AGREED by and between DSW Inc., by its duly authorized officers, and counsel for the Federal Trade Commission that:

1. Proposed respondent DSW Inc. is an Ohio corporation with its principal office or place of business at 4150 East 5th Avenue, Columbus, Ohio 43219.
2. Proposed respondent admits all the jurisdictional facts set forth in the draft complaint.
3. Proposed respondent waives:
 - A. any further procedural steps;
 - B. the requirement that the Commission’s decision contain a statement of findings of fact and conclusions of law; and
 - C. all rights to seek judicial review or otherwise to challenge or contest the validity of the order entered pursuant to this agreement.
4. This agreement shall not become part of the public record of the proceeding unless and until it is accepted by the Commission. If this agreement is accepted by the Commission, it, together with the draft complaint, will be placed on the public record for a period of thirty (30) days and information about it publicly released. The Commission thereafter may either withdraw its acceptance of this agreement and so notify proposed respondent, in which event it will take such action as it may consider appropriate, or issue and serve its

complaint (in such form as the circumstances may require) and decision in disposition of the proceeding.

5. This agreement is for settlement purposes only and does not constitute an admission by proposed respondent that the law has been violated as alleged in the draft complaint, or that the facts as alleged in the draft complaint, other than the jurisdictional facts, are true.

6. This agreement contemplates that, if it is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to the provisions of Section 2.34 of the Commission’s Rules, the Commission may, without further notice to proposed respondent, (1) issue its complaint corresponding in form and substance with the attached draft complaint and its decision containing the following order in disposition of the proceeding, and (2) make information about it public. When so entered, the order shall have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other orders. The order shall become final upon service. Delivery of the complaint and the decision and order to proposed respondent’s address as stated in this agreement by any means specified in Section 4.4(a) of the Commission’s Rules shall constitute service. Proposed respondent waives any right it may have to any other manner of service. The complaint may be used in construing the terms of the order. No agreement, understanding, representation, or interpretation not contained in the order or in the agreement may be used to vary or contradict the terms of the order.

7. Proposed respondent has read the draft complaint and consent order. It understands that it may be liable for civil penalties in the amount provided by law and other appropriate relief for each violation of the order after it becomes final.

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual’s email address; (d) a telephone number; (e) a Social Security number; (f) credit and/or debit card information, including credit and/or debit card number, expiration date, and data stored on the magnetic strip of a credit or debit card; (g) checking account information, including the ABA routing number, account number, and check number; (h) a driver’s license number; or (i) any other information from or about an individual consumer that is combined with (a) through (h) above.

2. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

3. Unless otherwise specified, "respondent" shall mean DSW Inc., its successors and assigns and its officers, agents, representatives, and employees.

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

- A. the designation of an employee or employees to coordinate and be accountable for the information security program.
- B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other system failures.
- C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.
- D. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows

or has reason to know may have a material impact on the effectiveness of its information security program.

II.

IT IS FURTHER ORDERED that, in connection with its compliance with Paragraph I of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
- B. explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the nonpublic personal information collected from or about consumers;
- C. explain how the safeguards that have been implemented meet or exceed the protections required by Paragraph I of this order; and
- D. certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of nonpublic personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP); a person qualified as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondent shall provide the initial Assessment, as well as all: plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relied upon to prepare such Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial

Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

III.

IT IS FURTHER ORDERED that respondent shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each document relating to compliance with the terms and provision of this order, including but not limited to:

- A. for a period of five (5) years: any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and
- B. for a period of three (3) years after the date of preparation of each biennial Assessment required under Paragraph II of this order: all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relating to respondent's compliance with Paragraphs I and II of this order for the reporting period covered by such biennial Assessment.

IV.

IT IS FURTHER ORDERED that, for a period of ten (10) years after the date of service of this order, respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having supervisory responsibilities with respect to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after the date of service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

V.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Paragraph shall be sent by certified mail to the Associate Director, Division of

Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VI.

IT IS FURTHER ORDERED that respondent shall, within one hundred eighty (180) days after service of this order, and at such other times as the Federal Trade Commission may require, file with the Commission an initial report, in writing, setting forth in detail the manner and form in which it has complied with this order.

VII.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

- A. Any Paragraph in this order that terminates in less than twenty (20) years;
- B. This order's application to any respondent that is not named as a defendant in such complaint; and
- C. this order if such complaint is filed after the order has terminated pursuant to this Paragraph.

Provided, further, that if such complaint is dismissed or a federal court rules that the respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Paragraph as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Signed this ___ day of _____, 2005

DSW INC.

By: _____
DSW INC.

WILLIAM C. MACLEOD
Collier Shannon Scott, PLLC
Counsel for respondent DSW Inc.

JAMES E. PHILLIPS
BENITA KAHN
Vorys, Sater, Seymour and Pease LLP
Counsel for respondent DSW Inc.

FEDERAL TRADE COMMISSION

JESSICA RICH
MOLLY CRAWFORD
LARA KAUFMANN
Counsel for the Federal Trade Commission

APPROVED:

JOEL WINSTON
Associate Director
Division of Financial Practices

LYDIA B. PARNES
Director
Bureau of Consumer Protection

052 3117

**UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION**

COMMISSIONERS: **Deborah Platt Majoras, Chairman
Pamela Jones Harbour
Jon Leibowitz
William E. Kovacic
J. Thomas Rosch**

_____)
In the Matter of)
)
NATIONS TITLE AGENCY, INC.)
a corporation,)
)
NATIONS HOLDING COMPANY,)
a corporation,)
)
and)
)
CHRISTOPHER M. LIKENS,)
individually and as an officer of)
Nations Holding Company.)
_____)

DOCKET NO. C-

COMPLAINT

The Federal Trade Commission ("Commission"), having reason to believe that Nations Title Agency, Inc., Nations Holding Company, and Christopher M. Likens have violated the provisions of the Commission's Standards for Safeguarding Customer Information Rule ("Safeguards Rule"), 16 C.F.R. Part 314, issued pursuant to Title V, Subtitle A of the Gramm-Leach-Bliley Act ("GLB Act"), 15 U.S.C. § 6801-6809; the Commission's Privacy of Customer Financial Information Rule ("Privacy Rule"), 16 C.F.R. Part 313, issued pursuant to the GLB Act; and the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Nations Title Agency, Inc. ("NTA") is a Kansas corporation with its principal office or place of business at 9415 Nall Avenue, Prairie Village, Kansas 66207. Respondent NTA is a wholly-owned subsidiary of respondent Nations Holding Company.

2. Respondent Nations Holding Company ("NHC") is a Kansas corporation with its principal office or place of business at 5370 West 95th Street, Prairie Village, Kansas 66207. NHC conducts business through its 57 wholly-owned subsidiaries, including NTA, in twenty states. During all relevant time, NHC controlled the practices at issue in this complaint.
3. Respondent Christopher M. Likens ("Likens") is president and sole owner of NHC, a Subchapter "S" corporation, and NHC's wholly-owned subsidiaries. He has the authority to control the conduct of NHC and its subsidiaries, including NTA. Individually or in concert with others he formulates, directs, or controls the policies, acts, or practices of the respondent corporations, including the acts or practices alleged in this complaint. His principal office or place of business is the same as NHC.
4. Respondents provide services in connection with financing home purchases and refinancing existing home mortgages, including, but not limited to, real estate settlement services, residential closings, title abstracts, title commitments, appraisals, foreclosure management, asset disposition, and real estate management. In providing these services, respondents routinely obtain sensitive consumer information from banks and other lenders, real estate brokers, consumers, public records, and others, including but not limited to consumer names, Social Security numbers, bank and credit card account numbers, mortgage information, loan applications, purchase contracts, refinancing agreements, income histories, and credit histories (collectively, "personal information").
5. Since at least 2003, respondents have engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for consumers' personal information. Among other things, respondents failed to: (1) assess risks to the information they collected and stored both online and offline; (2) implement reasonable policies and procedures in key areas, such as employee screening and training and the collection, handling, and disposal of personal information; (3) implement simple, low-cost, and readily available defenses to common website attacks, or implement reasonable access controls, such as strong passwords, to prevent a hacker from gaining access to personal information stored on respondents' computer network; (4) employ reasonable measures to detect and respond to unauthorized access to personal information or to conduct security investigations; and (5) provide reasonable oversight for the handling of personal information by service providers, such as third parties employed to process the information and assist in real estate closings.
6. In April 2004, a hacker exploited the failures set forth in Paragraph 5 by using a common website attack to obtain unauthorized access to NHC's computer network. In addition, in February 2005, a Kansas City television station found intact documents containing sensitive personal information discarded in respondents' dumpster in an unsecured area adjacent to respondents' building.

7. The acts and practices of respondents alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

VIOLATIONS OF THE SAFEGUARDS RULE

8. The Safeguards Rule, which implements Section 501(b) of the GLB Act, 15 U.S.C. § 6801(b), was promulgated by the Commission on May 23, 2002, and became effective on May 23, 2003. The Rule requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards’ key controls, systems, and procedures; (4) overseeing service providers, and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.
9. Respondents NHC and NTA are “financial institutions,” as that term is defined in Section 509(3)(A) of the GLB Act.
10. As set forth in Paragraphs 5 and 6, respondents have failed to implement reasonable security policies and procedures, and have thereby engaged in violations of the Safeguards Rule, by, among other things:
- A. Failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information;
 - B. Failing to design and implement information safeguards to control the risks to customer information and failing to regularly test and monitor them;
 - C. Failing to investigate, evaluate, and adjust the information security program in light of known or identified risks;
 - D. Failing to develop, implement, and maintain a comprehensive written information security program; and

- E. Failing to oversee service providers and to require them by contract to implement safeguards to protect respondent’s customer information.

VIOLATIONS OF THE FTC ACT

11. Since at least 2001, respondents NHC, NTA, and Likens have disseminated or caused to be disseminated to consumers privacy policies and statements, including, but not limited to the following:
- NTA, at all times, strives to maintain the confidentiality and integrity of the personal information in its possession and has instituted measures to guard against its unauthorized access. We maintain physical, electronic and procedural safeguards in compliance with federal standards to protect the information. (Nations Title Agency Privacy Policy.)
12. Through the means set forth in Paragraph 11, respondents have represented, expressly or by implication, that they implement reasonable and appropriate measures to protect consumers’ personal information from unauthorized access.
13. In truth and in fact, as set forth in Paragraphs 5 and 6, respondents did not implement reasonable and appropriate measures to protect consumers’ personal information from unauthorized access. Therefore, the representation set forth in Paragraph 12 was, and is, false or misleading, in violation of Section 5(a) of the Federal Trade Commission Act.

VIOLATION OF THE PRIVACY RULE

14. The Privacy Rule, which implements Sections 501-509 of the GLB Act, 15 U.S.C. §§ 6801-6809, was promulgated by the Commission on May 24, 2000, and became effective on July 1, 2001. The Rule requires financial institutions to provide customers, no later than when a customer relationship arises and annually for the duration of that relationship, “a clear and conspicuous notice that accurately reflects [the financial institution’s] privacy policies and practices” including its security policies and practices. 16 C.F.R. §§ 313.4(a); 313.5(a)(1); § 313.6(a)(8).
15. As set forth in Paragraphs 11 through 13, respondents disseminated a privacy policy that contained false or misleading statements regarding the measures implemented to protect consumers’ personal information. Therefore, respondents have disseminated a privacy policy that does not accurately reflect their privacy policies and practices, including their security policies and practices, in violation of the Privacy Rule.

16. The acts and practices of respondents as alleged in this complaint constitute unfair or deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this _____ day of _____, 2006, has issued this complaint against respondents.

By the Commission.

Donald S. Clark
Secretary

**ORAL STATEMENT OF
COMMISSIONER JON LEIBOWITZ**

before the
Committee on Commerce, Science, and Transportation
U.S. Senate
on
Data Breaches and Identity Theft
June 16, 2005

Good morning, Mr. Chairman and Members of the Committee.

We were all stunned to learn about the Citigroup computer tapes with customers' personal data that recently were lost during UPS transit. But what struck me most was a remark by one privacy advocate in a *New York Times* story. She said:

"Your everyday dumpster diver may not know what to do with these tapes, but if these tapes ever find their way into the hands of an international crime ring, I think they'll figure it out."

Let's hope by now these tapes are either buried deeply in a landfill – or they are soon recovered untouched. But the truth is that consumers' personal information is being compromised every day – and that the data security problem is not confined to U.S. borders.

Indeed, American consumers routinely divulge personal information to foreign websites. They routinely share credit card numbers with telemarketers from around the world. And they routinely receive spam from distant corners of the globe.

Let me share just a few disturbing scenarios with you:

- A foreign website selling to U.S. consumers states that "we take all reasonable steps to safeguard your personal information." In fact, the company takes no such steps and posts sensitive consumer data in a publicly accessible manner.
- Thieves from Eastern Europe use spyware to track U.S. consumers' keystrokes as they shop over the Internet.
- Overseas telemarketers obtain U.S. consumers' bank account information under false pretenses (that's called "pre-texting") and use it to wipe out their accounts.

Sadly, these examples are based on real FTC investigations¹ – many of which, unfortunately, are difficult to pursue because of limits on our ability to exchange information with foreign law enforcement partners.

Mr. Chairman, the Commission expects to issue a Report later this summer that details the harm caused by trans-national fraud and the serious challenges we face in investigating these international cases. Foreign law enforcement agencies may be unwilling to share information with the FTC because we cannot sufficiently guarantee the confidentiality of that information. And we are prohibited from sharing certain information we obtain in investigations with our foreign counterparts – even if they want to help us and even if sharing information would help stop fraud against U.S. consumers.

To be sure, there is no panacea for the problems of international data security breaches. But legislation allowing us to exchange information with foreign law enforcers under appropriate circumstances would be a significant step forward.

The bottom line is this: if you want the FTC to be more effective in stopping spam, spyware, and security breaches, you need to give us the tools to pursue data crooks across borders.

Mr. Chairman, I won't go into detail about the legislation. I know that you are looking at a draft of the bill, for which we are grateful. The draft is almost identical to the non-controversial measure Senators McCain and Hollings moved unanimously through your Committee and the Senate in the previous Congress. It still includes those minor changes made last year to address the concerns of industry and privacy groups.

Again, thank you for your willingness to listen to us today. Along with my colleagues, I'd be happy to take any questions.

¹ We have changed some facts to protect the confidentiality of our investigations.