FINAL TRANSCRIPT

Thomson StreetEvents℠

**ACCA - Records Policy Enforcement – Best Practices Across Corporate and E-mail Records

Event Date/Time: May. 19. 2005 / 1:00PM ET

CORPORATE PARTICIPANTS

Noel Elfant
Zebra Technologies - VP, General Counsel & Corporate Secretary

Jeff Hatfield
Jordan Lawrence - Director

Herb Wander
Katten Muchin Rosenman - Partner

PRESENTATION

Noel Elfant - *Zebra Technologies - VP, General Counsel & Corporate Secretary*

Hello, everyone, and thank you for attending the Association of Corporate Counsel webcast Records Policy Enforcement, Best Practices Across Corporate and E-mail Records. My name is Noel Elfant, and I am your moderator for today's program. I am also the Vice President and General Counsel and Corporate Secretary at Zebra Technologies Corporation.

Zebra delivers on-demand printing solutions for business improvement and security applications in 90 countries around the world. We manufacture and sell Zebra brand thermal barcode, smart label, receipt and card printers. We also offer software connectivity solutions and printing supplies.

Today's program will last approximately 50 minutes. At the conclusion, our presenters will answer as many questions as we have time for. I encourage you to submit questions to questions@jlgroup.com. Any questions we receive but cannot answer live today will be answered via return e-mail.

I have had the distinct pleasure to work with both of our speakers and their companies whom I would like to introduce now. Our first speaker is Jeff Hatfield. Jeff is a Director at Jordan Lawrence and plays a key role in helping companies establish and enforce legally defendable corporate records programs covering all record platforms. Jeff joined Jordan Lawrence in 1994 and has worked with senior management at over 300 national and international companies assisting in developing and implementing high impact records control solutions and systems. He is an accomplished speaker, has been published in numerous trade publications and conducts seminars for General Counsel, information management, audit and compliance groups. Jeff is an industry expert at banking, the legal community and Web services.

He is also a member of the Sedona Conference, a nonprofit research and educational Institute dedicated to the advanced study of electronic document retention and production. Jeff has more than 12 years experience as a records management executive. Prior to joining Jordan Lawrence, Mr. Hatfield was an executive with the Federal Reserve Bank of St. Louis responsible for the design and implementation of securities and item processing systems. Jeff received degrees in finance from the University of Missouri Columbia and Engineering from the University of Missouri-Rolla. He also holds an MBA in International Business Management from St. Louis University.

Our second speaker is Herb Wander who is a partner in the Corporate Law Department of Katten Muchin Rosenman where he concentrates on all aspects of business law especially corporate governance, securities law and mergers and acquisitions. As a member of an extensive list of associations, Mr. Wander brings knowledge, experience and networks to those he consults. He has been appointed to numerous committees and association boards that deal with corporate governance, audit matters and securities. In particular, Herb Wander was appointed co-chair of an advisory committee to the SEC to examine the impact of the Sarbanes-Oxley act on smaller public companies. He also is currently serving his second term as a member of the Legal Advisory Board of Governors, and he is a member of its Corporate Governance Subcommittee.

As an accomplished lecturer, Mr. Wander frequently speaks at institutes and programs in various business and legal organizations pertaining to corporate governance topics. In addition, he has published numerous articles and book reviews pertaining to

regulations and the practice of business law. Mr. Wander received a Bachelor's Degree from the University of Michigan and a law degree from Yale Law School. Following he obtained bar admissions from Ohio and Illinois.

Before we get started, I would like to set the stage for the material you will be hearing. I think everyone is well aware of the fact that records mismanagement has led to disastrous situations for many companies. We will be discussing a few of the more prominent examples today. I also think you would agree that it is now more critical than ever for companies to be able to consistently demonstrate that they have adequate controls and enforced policies in place that allow them to produce and protect needed records.

At Zebra, prior to working with Jordan Lawrence, we have the typical policies and retention schedules. We have operations in many parts of the world, so it was difficult for us to get our arms around developing a single control point that would ensure we were applying the necessary standards rules and controls for sound records management. Jordan Lawrence helped us improve our policies and processes.

I always tell people this is one of the most important things you can do to protect your company, but it is never at the top of anyone's to do list. We used to look at this effort as being an impossibly daunting task. However, having just been through one of these projects, I can speak from experience, listen to the information you receive today. These are absolute best practices that can help you get control of your records.

With that, I will turn over the program to Jeff Hatfield from Jordan Lawrence.

Jeff Hatfield - *Jordan Lawrence - Director*

Thanks, Noel, and thank you to everyone attending today. I want to start by sharing part of a recent interview with Judge Scheindlin who I'm sure you all know presided over the well-publicized case of UBS Warburg versus Zubulake. This interview was conducted and is copyrighted by the Sedona Conference. Judge Scheindlin was asked to assume for a minute that she had decided to leave the bench tomorrow and become the General Counsel of a Fortune 500 company. And she was asked, what would be the first 10 steps she would take to ensure that her company was prepared to comply with its discovery obligations with respect to electronic discovery?

And Judge Scheindlin said that at the top of her list would be to ensure that there was a well thought out records retention policy in place for business purposes that takes into account any statutory or regulatory obligations. Later in the interview when asked about Sarbanes-Oxley, Judge Scheindlin pointed out that the most notable changes that Sarbanes-Oxley makes for electronic discovery is to criminalize a broad array of conduct associated with the destruction of documents. And she also said that lawyers and senior management need to take a more active role in managing document retention plans from the very beginning. And our next speaker, Herb Wander will be discussing Sarbanes-Oxley in more detail.

Slide two. Judge Scheindlin's comments come as no big surprise. Never before have we seen a time in which records or more specifically the lack of enforced records policy has played such a significant role in the legal and public relations landscape that corporate America operates in.

Now bear in mind enforcing your records policy is not only about choosing the right technology. Instead it is about insuring that your company is able to consistently follow your published retention policy throughout all record storage locations and systems. Now once you have accomplished that, you can then select new technologies or make better use of the technologies you already have in the cases in which corporate record policies play a central role are abundant and the resulting fines and losses are staggering.

Just look at the Arthur Anderson case. A $9 billion company was brought to its knees because it did not enforce the policy it had regarding corporate records. Now we will review some of the other prominent cases later in the program.

Today it is seldom a case of a company not having a record management policy. It is more generally the fact that the actual policy, their actual practice does not reflect the policy. In fact, in a survey we conducted last year for the ACC the survey showed that 76% of the participating companies said they have a records policy in place, but only 18% said they actually enforced their policy. 80% of the companies with policies in place said they were less than satisfied with their current records program.

Records policies must be enforced systematically and non-selectively. Or to put it more simply, policy must be connected to practice. It is the same as it is in any other area of corporate governance, compliance or legal protection, and the risks and the costs are far too significant to ignore this any longer.

Slide three. Often at the beginning of litigation, many companies find themselves in the position of having to devote precious resources explaining discrepancies between their records policies and their actual practices, as opposed to really concentrating on the strategies of their case. In some instances, the merits of the case is obscured by records management problems. Companies are many times unable to produce records that they had but could not find. Or conversely companies cannot produce records that they should have but don't. As a result, businesses are being hit with fines, penalties and adverse judgments. It is also not uncommon for counsel to be unaware of records that are produced and maintained by their operations. So it's very difficult for them to execute an effective document hold process if they are not certain what records even exist.

Then there is e-mail. E-mail is such a hot topic today, and you can almost daily pick up the paper and read an article related to e-mail and litigation or government investigation. Many of you probably saw the article on the front page of Monday's Wall Street Journal. The title was, "How Morgan Stanley Botched a Big Case By Fumbling E-mails."

Companies just like Morgan Stanley are throwing millions of dollars at this issue, and it does not seem to be making a difference. In regards to e-mail, technology by itself is ineffective because regardless of the investment in supporting technology employees can and do work around the policy. You must have clearly defined standards, rules and requirements set and enforced in order for these technological solutions to work. Policies must be enforced, along with consequences for employee noncompliance.

Perhaps two of the most common and dangerous positions to be in are when companies cannot explain why their records policy states one thing and their actual practice shows something else or when they cannot protect records that are subject to legal or examination hold requirements. Each of these situations create the appearance of selectivity, inconsistencies and possible wrongdoing on the part of the company.

Slide four. Today I'm going to cover five topics. The first is the basic records related requirement all companies must meet. Secondly, we will look at the minimum records related information that makes records policies enforcement possible, and then I will discuss an overview of how a company can integrate policies into practice, or said a different way how you can ensure your tactical solutions operating in accordance with your strategic initiatives. And finally, I will summarize some of the keys to ensure your minimizing risks related to record management.

Slide five. In order to protect your company's corporate interest, you must be able to demonstrate consistency in meeting four very basic requirements. First, you must be able to demonstrate that you keep records long enough to meet retention requirements. It is critical that you not only consider the legal and regulatory requirements, but also the valid business and operational requirements, your tax needs, as well as industry standards for retaining records.

Second, you must be able to locate records quickly and effectively when needed. When records are required for examination or litigation, you must be able to produce them if you have them regardless of where they are or how they are maintained. And the courts and regulators today are becoming less and less tolerant of delays.

Third, you must be able to destroy records consistently and non-selectively when they become obsolete. Almost all records become obsolete at some time, and it is in your best interest to destroy them. If records exist and they are requested, they must be produced regardless of when they could have been legally destroyed.

Now at some point, records cease to be assets. They become liabilities. They increase your risks and your costs, not just storage costs but also the cost of unnecessary research and production, the cost of data maintenance and data conversion. But when destroying records, however, be absolutely certain to do it in a consistent, nonselective and well-documented manner.

And finally, you must have the ability to enact immediate and verifiable records holds when the records are needed for litigation or examination. Now this is perhaps the most important requirement, and this is the one requirement that so many companies have been unable to meet and it is the one that has caused so many of the fines, sanctions, obstruction charges, adverse inferences and lost litigation.

So these are the basic requirements, and they apply to all areas of the Company and all records media types. You must be able to demonstrate that your Company meets these requirements consistently, and you must be able to show that your policy is connected to practice.

Slide six. But the only way to ever ensure you are meeting these requirements is to have four critical pieces of information about your records. You must know what types of records your company generates and retains. It is rare that we find companies that actually have clear standard of classification across the entire enterprise and can easily identify needed records.

Last year's survey of ACC members showed that 86% of the companies do not have standard record classifications identified and applied to their records. You need to know who owns and controls records. You must know who owns and controls records in order to ensure that they can be produced, that they can be protected and destroyed as required. This applies to both official records and copies of records.

Our survey showed that 42% of companies could not identify the owners of their records. You need to know where records are located. This includes knowing where they are geographically and on what media types and in other locations like IT managed systems. Only 20% of the companies in the survey said they could actually locate records when needed.

And finally, you need to know when records can be destroyed because they have fulfilled any regulatory or valid business needs. Only 48% of the companies said they were consistently applying their records retention requirements to their records in order to accurately calculate destruction requirements. 73% of the companies said they allow their employees to destroy records as needed without validation of consistency or non-selectivity.

Again, these are the types of information you need to know about your records. To have an enforced records program, this information must be captured and standardized, and it must be controlled and accessible centrally and then applied to all media types in all areas of the Company, and it must be regularly updated. And this is what creates a single windowpane through which you can access records when needed so that you can know what you have and what you don't have, and so you can know how to get to the records and know how to protect them.

Let me give you an example I think will tie this together. We recently completed a project for a Fortune 100 company. Now one of the initial steps we take a client through is a series of what we call profiling sessions. We do this at the division level, and it is where we identify all of the relevant information about their records. Like I said, our survey showed most companies do not have standards applied to their records. This company was no different.

According to their records policies and retention schedules, they had over 7000 different types of records. However, through a process of binge-marking record types against industry standards by compressing logical document groupings into records classifications and identifying redundancies, the client was able to reclassify records into less than 1200 standard record types for both paper and electronic records. These types of results are typical. Furthermore, like many companies today, this company was grappling with e-mail. Their legal and IT departments were locked in a seemingly endless series of meetings trying to find the right technological solution that would bring some structure to e-mail management without impeding their business.

Now in light of all the hours they had invested in the e-mail issue, this company was lacking some critical information about their e-mail records. They did not know how their employees used e-mail and what records were actually being communicated via e-mail and why.

Now keep in mind most generally accepted studies today have shown that at least 80% of e-mail within companies does not serve a specific business purpose. It is typically nonbusiness essential communications. Our clients found that fewer than 100 types of business e-mail records were actually required to be retained. They identified these on the retention schedule and set the relevant requirements and then developed an enforceable e-mail policy.

This effort had nothing to do with the volume of e-mail. Instead, it was a deep down look at how the business was actually using e-mail and what was important. So you cannot really begin to get your arms around e-mail until you first understand how to e-mail is being used at the departmental level.

So with all this information, this client was now -- had to have the framework for an effective and practical records control program. All the critical information that was required to enforce the policy is now included in the records retention schedules companywide. Records policies and related requirements are monitored and enforced through a central control point.

Slide seven. One of the biggest mistakes we see companies make when addressing records policies and records programs is that they skip the strategy development and jump right into tactical solutions. Just as you would do when developing and implementing any other corporate governance initiative, you must first have a solid strategy in place before you set out to determine tactical needs and solutions.

Now the strategy part of records controls includes things like documentation. Documentation includes your records policies, retention schedules, enforcement notices, notices that are specific instructions to the rest of the Company for records-related activities like destruction and protection due to the legal hold orders. It also includes the documentation that validates compliance. This documentation must be developed with a clear understanding of all the requirements -- the records ownership, location and so on -- those four pieces of critical information we just discussed. This documentation must also match what is actually happening within your company.

This leads us to the second part of the strategy setting which is the record type profiling. Record type profiling, as I said earlier, includes gathering and standardizing all records-related information -- the what, who, where, and when. It is also helpful to determine the record type usages, volumes, access patterns and costs. This additional information helps you make better decisions regarding your tactical solutions.

Strategy should also include the development and implementation of some form of automation to manage your documentation and your standards. This type of automation should become your central hub for monitoring records controls for accessing records through research, for managing legal hold requirements and making ongoing program updates and so on. And finally, any compliance, legal or corporate governance related policies must be audited and validated on a regular basis.

So having a good strategy set from the beginning is what will allow you to make that critical connection from policy to practice. A strong practical well thought out strategy will enable you to better leverage your tactical solutions.

On the tactical side of records control, this includes all the various storage systems and facilities. It includes e-mail archiving systems, content management software and so on. On average, our clients operate with 120 different tactical solutions. These tactical solutions must have the standards, the rules and the requirements applied in order to ensure that they are helping you stay in compliance due to legal risks and costs, as well as improving access and control. So set your strategy first, then integrate your policy with the tactical solutions that are tasked with executing the policy.

Slide eight. In addition to setting and applying records-related standards and strategies, there are several important areas of risk mitigation that I wanted to cover briefly.

Regulatory tagging. With so many regulations related to retention, production, security and general disposition of records, it has become critical for companies not only -- that they not only know what record types they have, but they also have tagged an impertinent regulatory requirement against relevant records. This should occur during the collection of critical record type knowledge, those profiling sessions I talked about.

Secure destruction requirement. Many records-related regulations now stipulate specific forms of secured destruction for which you are expected to comply with. Just as you must tag record types with regulatory retention requirements, you must also tag your appropriate record types with secured destruction requirements.

Notifications and responses. As I said earlier, notifications should be used to communicate instructions concerning records retention, disposal and protection, and these notices must be sent out consistently and at set frequencies to your employees, your departments and any of those tactical systems retaining records. The key to this process, however, is the validation that the instructions have been carried out. This is accomplished by requiring compliance responses to each one of those notices.

Legal hold process. Legal holds are critical. Herb will discuss this from a litigator standpoint. In short, however, counsel must have the ability to enact immediate and verifiable holds on records across the Company and across all the various processes that manage your records. You must be able to identify the records that are needed and notify the correct people, the correct locations, as well as IT and give them the details about the records that need to be protected. Your compliance responses are critical for a successful legal hold management and tracking.

Auditable events. You must ensure that each of these items listed here are creating auditable events that can be documented. They can be verified and followed up on to ensure your risks are mitigated. This is your CYA so to speak.

And finally, no matter what level of automation you use enforcing records policies will always require employee behavior modification. There is just too many areas within your company where records are under the the direct control of your employees. Employees must be consistently trained on their records-related responsibilities, the expectations and the consequences for noncompliance. Again, just like you would any other area of corporate governance. Most of our clients require employees attend records-related training at least annually and have certified that they understand the enforcement of the policies. Many of them have added this to their ethics and other training curriculum.

Slide nine. In conclusion, I would like to summarize by stating that our experience is that most corporate counsel are in agreement that policy development and enforcement is critical. In that survey last year, the survey showed that 65% of the companies ranked litigation and discovery as the top risks related to record management. Our experience has also shown that establishing an enforced records policy and control program is not too terribly difficult to accomplish, and it is well worth the effort from a corporate governance, a risk reduction and a cost savings perspective. The companies that enforced practical corporate records policies unquestionably reduced their legal and regulatory risks. They have the records that they need to have, they are able to produce and protect them quickly, accurately and effectively, and they do not over retain records.

Policy development is important, but enforcement is where all the benefits are. So there is plenty more to discuss, and I encourage you to contact us for any more information. But for now, I will turn the program over to Herb Wander for his discussion of post Sarbanes-Oxley corporate records management.

Herb Wander - *Katten Muchin Rosenman - Partner*

Thanks very much, Jeff. It is a pleasure to be with you this noon hour today to discuss this very very important topic which all of you who read the papers this morning can see how important it can be with the $800-some million punitive damages that the jury awarded Mr. Perelman against Morgan Stanley this morning, or yesterday.

Before we get to Sarbanes-Oxley, let me guess indicate a few basic rules about documentary retention and destruction. These are required by federal laws, by state laws and regulations from various government agencies. There are also business needs that require you to maintain documents such as indentures, while there is still debt outstanding under them, or to maintain deeds over a long period of time.

So we both have federal, state, regulatory requirements, as well as business needs. You may need these documents as I say in the next bullet-point for affirmative purposes. You want to sue someone for breaching a contract. Do you have the support to go into court to show what the contract meant and how it was performed or how it was not performed, so that your lawyers are given a real good opportunity to pursue legal rights against someone else.

It is also necessary as a defensive response to discovery request against someone who might be suing you or against an investigation by some regulatory agency or even a criminal group such as the U.S. Attorney, Postal Inspectors or the FBI. And as Jeff has said, good recordkeeping makes good business sense.

The next slide, please. Actually the new environment was not created by Sarbanes-Oxley, but, in fact, the environment created Sarbanes-Oxley. But the real impetus for one of the reasons for Sarbanes-Oxley, as you all know, was all of the corporate scandals, particularly Enron and then WorldCom broke the camel's back. But as part of Enron, I think all of us are familiar with the indictment of Arthur Anderson which eventually forced them to discontinue business and go into the liquidation mode. That was essentially caused by the destruction of documents. I just saw the other day the movie Enron, the documentary, and they actually have movies of big, big, big bundles of destroyed documents being burned after they had been shredded.

Arthur Anderson, as you know, the case was argued in the Supreme Court probably about six weeks ago, and in fact, it may be overturned. But the damage has already been done. Well, all those scandals and the destruction of documents were the basis for the enactment by Congress of Sarbanes-Oxley. And actually only one provision of Sarbanes-Oxley deals with the destruction of documents, and I put that in the slide at Section 1102.

It is very simple. It says whoever corruptly alters, destroys, mutilates or conceals a record document or other object or attempts to do so with the intent to impair the object's integrity or availability or otherwise obstructs justice in any way shall be fined or imprisoned not more than 20 years. You can see that 20 years was a big increase over previous statutes.

Now this is essentially the section that deals with all the public companies that are governed by Sarbanes-Oxley, and it does not deal with the specific sections dealing with accountants, and there are some special ones that we will not have time today to go into.

The next slide, please. The new environment for document retention and destruction, and let's look at some of the effects that we are presently experiencing. Both government and also state regulatory agencies are conducting many many investigations today. In fact, there is a new term that the SEC uses, it is called prospecting. They don't really get a complaint from someone, but they feel that there is something amiss in a particular industry, and they will go out and send subpoenas to people and say, tell me about all your customers and suppliers and whether -- and ask for documents with respect to them to determine, for example, whether a particular company has in effect conspired with a customer or supplier to enable that customer or supplier to manipulate its revenue recognition policy.

For example, agreeing to buy product with a side letter that says we can return the product later if we don't like it, whereas the seller of the product would book that revenue, which was a violation of Generally Accepted Accounting Principles.

Another example of where a document retention and destruction is so important are with respect to audit committees today, and let me give you a typical example of what may happen when a company experiences a restatement of its financial statement. During the process that leads up to the determination to make a restatement, the accounting firms are now required to do an extended audit to determine whether there has been any fraud exposed. It is called a SAS 99 review. And frequently the auditing firms will send in their forensic accountants to determine whether there has been fraud or manipulation or intent to manipulate

the financial results of the Company. The forensic accountants will generally do an e-mail search, and they will give various protocols to the Company to search all of the e-mails and all of the electronic documents that it has, and they will be given words like cushion, accelerate earnings, things of that sort, that they suspect may have happened.

As a result, if they come up with some of these e-mails, and it only may be a handful out of literally a million documents, they then will go to the audit committee and suggest that the audit committee retain independent outside counsel, probably of forensic accountants, and conduct an investigation to determine whether someone, in fact, did manipulate the financial statements. Those searches are not just searches of the accounting records as I said, but they are searches of all of the electronic documents, and in particular the e-mails, and that is from both vendors and receivers. It is a long, costly and very very difficult process. And as I think we all know, people tend to use e-mails in a very flippant and casual way rather than as a business document, and as a result, many times things are said in a hurry that are not very well explained and then can lead to further investigations, costly investigations, both in terms of the cost of the investigation, as well as the time that it takes. And as a result, you could just go through mountains and mountains of documents.

Special litigation committees are formed if a company is sued derivatively, and independent directors are appointed to determine whether the company should process prosecute the lawsuit itself or whether it should ask for dismissal of that lawsuit. And again, having the records available here generally speaking in an affirmative sense will enable that special litigation committee to determine whether they will recommend that their lawsuit be dismissed.

There are special committees just for general investigations, as well as there is documents called for in all sorts of litigation. In fact, I heard the President of the American Bar Association speak last week here in Chicago. He is the first one I have heard locally say that perhaps we actually do too much discovery, and there are so many documents available it is becoming so costly and does not automatically produce the truth when you get the warehouses full of documents.

And finally, I would be remiss if I did not mention internal controls under Section 404 of Sarbanes-Oxley. As most of you know, public companies either have been required or depending on their size will be required to have an internal audit done by the management and then have that internal audit attested to by the independent accountant. The independent accountant will also do its own audit of internal controls. And what has happened here is that the new public accounting oversight board has in its rules governing this internal control has insisted and emphasized that everything must be documented. Everything must be documented -- all the controls, all the results, all the tests. They have imposed that on the public accounting firms, and the public accounting firms have turned around and imposed that same requirement on their own audit clients so that almost a new industry is, in fact, growing up today where in order to satisfy the internal control requirements of Sarbanes-Oxley, the accounting firms have to maintain documents that they did everything in connection with their audit and what they did, as well as the companies themselves are having to maintain very extensive documentation.

I might add that the whole basis for internal controls comes from the COSO report, which itself did not emphasize as much as the PCA, OB or the accounting firms to maintain documents. But that is the aftermath of all the scandals and the adoption of Sarbanes-Oxley.

The next slide, please. What are the features of the new environment for document retention and destruction? As Jeff has said and I'm not going to go into this in great detail, but the fact is when litigation ensues, they are not going to be able to then say, oops, I have got to go back and implement my document retention and destruction program, and all these documents should have been destroyed so I'm going to destroy them. Once there is litigation, criminal investigations, things of that nature, there must be a hold on these documents. You don't have catch up time to implement the process that you have adopted but have not followed.

Secondly, the courts more and more and the regulatory agencies in particular are emphasizing fast and complete document production.

The third point is that there is, as I said earlier, an emphasis on electronic discovery including e-mail. So all these records are searched. It seems to me sometimes impossible of have anybody go through all of them there are so many, but as I said, there are search protocols that supposedly will smoke out the damaging document. And, in fact, there is no stonewalling really that government agencies or courts will condone in today's world as we have seen in some of these cases that I'm now going to turn to on the next slide.

These are sort of the stories that we have all seen in the paper. The Bank of America fined $10 million by the SEC for failure to produce documents. The UBS Warburg, somewhat similar case to the Morgan Stanley case, where they were not able to produce the e-mails, and the jury was awarded the plaintiff's $29 million.

Phillip Morris had the same problem, and Frank Quattrone, who has been convicted, the former head of investment banking for high-tech companies for CSFB was essentially convicted for, as we say here, the e-mail, again e-mail notice. Cleanup those files. As you probably know, he went through two trials and on the second trial was convicted. And he is appealing that.

The next slide deals with the real headline that we have all been reading the last week or so, and that is the Morgan Stanley case. When I put together these slides, the decision was not in. But as you probably all know, they were hit with the $604 million judgment in the fraud suit by Mr. Perelman, and yesterday the jury came in with an $807 million punitive damage award. And the reason that this happened is because of what the judge considered to be stonewalling and failing to comply with court orders on discovery, and the judge got so fed up with this, and I'm basing all this on the newspaper reports, which I think have been fairly uniform in this area, that the judge got fed up with it and said, and I'm going to tell the jury that they should presume that the plaintiff has proven their case, and that the defendants now have the burden of in effect disproving. So that turning the burden of proof around, and I think all of us who have ever been in court knows that the burden of proof can be the determinative factor in a great many cases, and it appears to have been so here. So now Morgan Stanley has got an over $1 billion judgment outstanding against it. Morgan Stanley indicates that they will appeal, which I'm sure they will.

But this essentially was the result of incomplete document disclosure in an untimely fashion at least according to the judge, and Morgan Stanley's problems are not over because now everybody else who reads this in the newspaper that has ever had litigation with Morgan Stanley says, well wait a minute, I asked for discovery and maybe I'm in the category of not having the discovery properly produced to me. You will see that on the next slide.

And the SEC, according to newspaper articles, is considering commencing an enforcement action against Morgan Stanley for failing to retain e-mails and violating 2002 cease and desist order. So these are as Morgan -- these are like with respect to Arthur Anderson, can be do or die situations for a company.

The next slide, please. So what do you have to do with respect to document retention after initiation of an investigation? I will go through this quickly. You have to identify the relevant subject matter. You have to implement a litigation investigation hold. You have to identify the potentially relevant universe of documents. You have to gather them. I think as Jeff emphasized before, employee training is very important, and I think employees should clearly be told that this is a very serious matter and that they have to act quickly and honestly with respect to it. They have to maintain close supervision over them. The documents have to be reviewed, and they also have to be reviewed for -- some of them may contain attorney/client or work product materials that should be withheld from the discovery process.

Where do you locate these documents? This is the next slide. There are obviously paper files and documents, but people who have never had a subpoena before, they get all excited when they say well, we want your desk diaries, we want your calendars, we want your written notes, etc., etc.. And the discovery requests are so broad it is almost every document. And many laypeople and corporate officers and employees are quite surprised when they are asked to produce, for example, their calendars and notes.

We have already talked about e-mails and electronic materials, computer backup tapes, other electronic files and databases and, in fact, snapshots of Web pages. I can tell you from my own personal experience dealing with government agencies, if you

are slow in producing these documents or if you indicate you cannot find them or you cannot resurrect them, or there is a glitch in the tapes, right away the first thought of the investigator is, uh-oh, there is something fishy here. So then you become under even greater scrutiny, and it makes the whole process of the investigation much more difficult for your client, because of the Doubting Thomases from the investigative slide who today's world don't count non-production or slow production.

The last slide is just to emphasize to you this growing problem with e-mail. It has become so casual and so pervasive that the records are all over -- everybody has them. People are not very careful in what they say, and they are becoming the smoking guns in today's world. And having retention programs so that you can sift through the important business documents that are on e-mail and those that are not business documents that may be destroyed in a relatively short period of time, is crucially important as well as I cannot overemphasize really dealing with employees in terms of their use of e-mails and the fact is that these can be used infrequently or used against a company in all sorts of investigations and litigation.

And with that, I will conclude and am available for the question period.

QUESTIONS AND ANSWERS

Noel Elfant - *Zebra Technologies - VP, General Counsel & Corporate Secretary*

We do have questions, and I'm going to read the questions now. And the first question we have I will direct to Jeff, and Herb, you can certainly add into anything Jeff might have. The first question is as follows.

I'm in the process of revising our document management procedure, and I am interested in your thoughts on the retention of correspondence, i.e. daily e-mails exclusive of those items that are subject to specific statutory and regulatory retention requirements or to a litigation hold.

For instance, what are other companies doing in terms of enforcing a correspondence category? Do they have them? How do they make retention of such an ill-defined category a practice rather than just align in the procedure?

Jeff Hatfield - *Jordan Lawrence - Director*

This is Jeff. That is a very common issue with a lot of companies. Our clients I would say almost all of them do have something called correspondence, and they have it on their retention schedules, it is part of their policies and procedures. Now the requirements for retaining correspondence might vary from one area of the company to the next, but they don't have much risk and other types of issues that they see surrounding that type of correspondence.

But it is, indeed, well-documented, and here again, like I said, employees ultimately have control over a lot of the records. And correspondence is one of those. So this is something they have to handle through training, through those series of notices that I talked about, especially if it is in e-mail.

What we find with most of our clients is that they are working with IT to implement other types of controls like Auto Delete. I think the average right now is anywhere from 30 to 180 days. After an e-mail becomes that age, it is automatically deleted provided that it is not representing a true business need, in which case it will be pulled out of the group that gets auto deleted.

So correspondence definitely have that included. It should generally be a very short retention requirement. And then to follow on that, with training and routine auditing of the departments, it does not happen overnight. It is not something magically that you can say okay, we have got it taken care of. But it does require some certain steps and some diligence to make sure that it is managed properly. Herb, your thoughts on that?

Herb Wander - *Katten Muchin Rosenman - Partner*

Well, the only thing I would add is that you have to be careful if you're in some regulated industry that requires you to keep essentially all documents. Therefore, you just cannot get rid of it.

I was with an investment manager the other afternoon who said that they just gave up and said we are going to keep everything for 20 years. Now I don't know if he really meant 20 years. So you may not have the luxury of being able to sift through to determine whether some things are business records or nonbusiness record.

Noel Elfant - *Zebra Technologies - VP, General Counsel & Corporate Secretary*

Well, that somewhat dovetails a bit with the next question which is for you, Herb. And that is, do you know of any special rules related to government research documents retention? This is coming from a small research firm that does research writing publications and some Web support for the National Cancer Institute.

Herb Wander - *Katten Muchin Rosenman - Partner*

I don't. If the person wants to e-mail me, I know some people who are sort of expert in this area that I could put you in touch with, but I frankly have not had that come across my desk.

Noel Elfant - *Zebra Technologies - VP, General Counsel & Corporate Secretary*

I think what we could do, Jeff, is probably forward this e-mail to Herb, and he can respond if he has got someone he could refer.

Herb Wander - *Katten Muchin Rosenman - Partner*

Sure. Absolutely.

Noel Elfant - *Zebra Technologies - VP, General Counsel & Corporate Secretary*

The next question I will pose to Herb first, but Jeff you're welcome to add to it. Is there a line of demarcation between what appears to be an empty threat of litigation and being on notice of litigation for purposes of putting a hold on document destruction?

Herb Wander - *Katten Muchin Rosenman - Partner*

You can make that judgment, but I think in today's world everybody is so cautious that they are bending over backwards to try and maintain the documents. And the reason is it is just -- in today's climate, it looks like you had something to hide. And consequently even in sort of these frivolous claims, people are holding onto documents.

Jeff Hatfield - *Jordan Lawrence - Director*

I think I would add to that yes, absolutely. And as Herb and I both described, the process of identifying what should be placed on hold and actually carrying that out it really comes back to you have to be able to find the records you need, know what you have, know what is pertinent, know who to contact.

We see a lot of clients that will look at the records that they have within the organization and just like I said tag them according to different regulatory requirements. They will also tag them according to their experience and what is needed to be retained for legal matters and in terms of their risk. So a lot of times we talk to clients about what their requirements for retaining records are, and based on their past experience, they may decide, you know what, this is something that has come up in the past. I think we want to put some different requirements around this all because of what their spread or typical notices of litigation have been in the past.

Noel Elfant - *Zebra Technologies - VP, General Counsel & Corporate Secretary*

Okay. Let's get to the next question, which is this one will be for you, Jeff. If you were just starting a records retention program, how do you analyze and review the potentially hundreds of thousands or maybe millions of electronic documents that already exist on your employees' computers?

Jeff Hatfield - *Jordan Lawrence - Director*

Good question, big problem. The way we approach it is to start and get your standards and requirements set first and then start applying that to like the person said, the hundreds or even thousands or millions of records that are out there. It makes it much more simple. If you know what your requirements are, if you know what types of records you should be retaining and then you go out to the vast areas that are retaining those records, it makes the job much much quicker. You can even be looking at a lot of records that based on what you know about your requirements don't even have to be retained. So rather than trying to decide how should we -- where should we put them, how should we keep them, they can be eliminated immediately. And again, when you go to that microlevel that you really are talking about employee control and you have to go back to the things that Herb and I discussed earlier as far as educating, training and notifying people of what their responsibilities are.

Noel Elfant - *Zebra Technologies - VP, General Counsel & Corporate Secretary*

Okay. Another question for you, Jeff. Among companies that are doing it right, do you find that they have had to modify their backup procedures pretty significantly in order to do -- to more easily destroy documents on time without affecting other documents that have a longer retention time?

For example, if some documents are required to be kept for a year and others are required to be kept for two years, if companies are relying on backup media for the recovery of those documents, then it will be easier to store them on separate tapes so that the entire tape can be overwritten or destroyed when the data on the tape needs to be destroyed. To avoid having huge backup media management issues, have companies embarked on a policy to keep these retained documents online and are using backup media only for disaster recovery, which may mean that they are only able to restore from backup media for a period of 30 to 90 days?

Jeff Hatfield - *Jordan Lawrence - Director*

Good point. Excellent question. We do see that happening. We see fewer and fewer companies actually backing up the so-called archived records, and they are doing it online and other different media. If you do have -- well, two types of backups. If you have the backups like was mentioned for the disaster recovery where you're going through your normal rotation, that is fine. We don't see a lot of changes there other than just to make sure that when litigation comes up and you are required to place a hold on that, that you are looking at those backup tapes even if they are simply for disaster recovery and they get swapped out frequently.

The other type, the backups that are being retained for longer period of times, maybe a period of years, maybe it is your year-end backups that are retained for archival purposes, we do see a lot of companies that are modifying that procedure just as the

question suggested. They are partitioning that out so that everything that has a one year requirement goes to one year backup. Things that have a two-year go to another and so on.

The complexity and the significance of that is obviously going to vary depending on your systems and your circumstances, but if you don't do that, you do run into this situation where you're retaining far more information than you need just because certain pieces of information that will have backup you have to retain for a longer period of time than others.

Noel Elfant - *Zebra Technologies - VP, General Counsel & Corporate Secretary*

Okay. Well, it is about 1:00. I want to thank Jeff Hatfield and Herb Wander for participating in this program. Thank you, everyone, for submitting questions and participating.

Before we wrap up, I just want to remind everyone that the webcast has been recorded and will be available on the ACC website, and the transcript will also be available tomorrow at www.JordanLawrence.com. So again, thank you, everyone.
