A Global Perspective on Preventing Employee Data Theft and Trade Secret Misappropriation

Scott A. Holt
Cally M. Kothmann
David Morgan
Sivabalah Nadarajah
Cheryl A. Soloman
Cathy J. Testa

One of the greatest challenges facing companies globally is the theft of intellectual property. Virtually no business, anywhere around the world, is immune. As stated by U.S. Attorney General Eric Holder, there are only two categories of companies affected by trade secret theft — "[T]hose that know they've been compromised and those that don't know yet."

Lost revenue resulting from theft of intellectual property alone makes this problem too significant to ignore and, as such, a top priority for corporate counsel. In 2013, the U.S. Report of the Commission on the Theft of American Intellectual Property estimated that the U.S. loses more than $300 billion a year.[1]

While some of these thefts are the result of foreign and domestic competitors, an increasing percentage can be traced to employees within companies. A survey conducted by Symantec – a data security, storage and systems management provider – demonstrated how serious employee trade secret theft has become.

The Symantec survey covered employees who worked in corporate information technology, finance and accounting, sales, marketing and communication and human resources, who recently lost or left a job. The findings showed that a large percentage of these employees removed or accessed data improperly:

- 79 percent of respondents took data without an employer's permission
- 53 percent of respondents downloaded information onto a CD or DVD
- 42 percent downloaded information onto a USB drive
- 38 percent sent attachments from work to a personal email account
- 82 percent of respondents said their employers did not perform an audit or review of paper or electronic documents before the respondent left his/her job

Although trade secret theft can frequently be tied directly to employee and ex-employee actions, corporate policies and procedures are often not up-to-date or comprehensive enough as illustrated by this statistic from the Symantec survey:

[1] http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf

- 24 percent of respondents stated they had access to their employer's computer system or network after their departure from the company.

Today's interconnected economy, dominated by multijurisdictional concerns and their myriad strategic service partners, means that mission critical data is constantly circling the globe and being accessed and potentially mishandled by employees from Des Moines to Dubai.

The Employment Law Alliance, the world's largest network of labor and employment and immigration law firms, surveyed its members to assess this growing concern.

In Europe, the majority of countries we report on present a consistent theme of contractual intervention to deal with employee data theft and breach of confidential information. At a basic level, trade secrets and confidential information can (and should) be protected by employers through express terms in employment contracts.

Statutory provisions exist in some member states and the European Union has issued principles of "data protection." However, the clear message is that employers need to protect their business interests through clear contractual provisions. This is highly topical as new trade secret laws originating from the EU are being introduced this year that will clarify and reinforce existing laws of confidentiality for business information. The European Commission has recently recognized the growing importance of protecting confidential business information, in particular trade secrets. It estimates that 25% of companies reported theft of information in 2013, a 7% increase on the previous year. Fully entitled the "Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure," the proposals aim to implement a statutory framework that will provide an equal level of protection throughout the EU.

In Asia, it is the norm for companies to formulate their own in-house policies which cover access and usage of company equipment and data apart from the employer prerogative of physically securing IT assets such as servers and data rooms. It is notable that non-compete agreements are largely unenforceable in several major jurisdictions. However, trade secrets and confidential information are generally protected by specific legislation and companies can seek injunctive relief and damages for breach of contract

Looking at the issue of protecting trade secrets from a macro perspective, a recent survey conducted by the Ponemon Institute shed light on why data theft by employees is so widespread. This survey, which based its responses on 3,317 individuals in six countries, including the U.S., United Kingdom, France, Brazil, China and Korea, found that a majority of employees did not believe taking company data was wrong. A significant number also stated that their employer did not enforce its data protection policies, or that the employer's information was not secured and, frankly, readily accessible.

Various technological and workforce influences continue to shape the dynamics of this issue. The growing prevalence of BYOD or "Bring Your Own Device" and the ease and speed with

which employees can move information across multiple applications make it more arduous for companies to monitor and secure their data and intellectual property. Moreover, the increase in employee mobility and frequency of job changes, including those pursuing job opportunities in other countries, makes it more difficult to enforce laws designed to curb unfair competitive activities and protect intellectual property rights.

Understanding the patchwork of regulations and the various civil and criminal remedies available to employers dealing with trade secret theft is crucial.

Preventative Measures Regarding Employee Data Theft and Trade Secrets

In the U.S., companies are well-served in adopting "need to know"/"need to access" protocol. Restricting the ability of insiders to gain unauthorized access to confidential information can help limit unwanted removal or misappropriation of sensitive data. In addition to policies and procedures, the ability to detect and report internal breaches is mission critical.

Restricting internal access reduces the ability for employees to take company information with them whenever they are away from work or their employment has been terminated. If an employee doesn't need access to certain areas of information all of the time, consider restricting them from access as soon as they have the data they need. In addition, all access to confidential data in computers or on media devices should be password or copy protected and/or encrypted.

Data loss prevention tools can be used to identify, monitor and protect data in use, data in motion on the network and data at rest in the data storage area or on desktops, laptops, mobile phones or tablets. Network-based tools monitor data flow and, in some cases, filter or block data movement. Host-based tools monitor static data on systems and, at times, block or control actions that employees can remove. Technology is also available that analyzes file access and usage patterns on networks and servers.

Informing employees of their responsibility to be stewards of mission critical data and detailing the concerns through substantive training programs addressing trade secret protection policies and procedures is vital. Trainings need to be held at least annually with attendance mandatory.

Imbuing a sense of purpose to the organizational mission of safeguarding data engages employees and can lead to a generation of meaningful suggestions that help policies evolve. In addition, by setting expectations and providing a reporting mechanism, companies can increase the likelihood of detection of trade secret theft.

In addition to training, new employees should be required to sign all of the company's standard non-disclosure agreements and, if applicable, non-compete agreements. Employee orientation should include, at a minimum:

1. Overview of the company's trade secret policies.
2. Inquiry as to whether the employee possesses any confidential information or documents from a prior employer.
3. Inquiry as to whether the employee has any existing confidentiality agreements and/or non-compete agreements with a prior employer.
4. Instruction to the employee that he/she may not reveal any trade secrets or confidential documents obtained from a prior employer during the course of his/her employment with the company.

If the new employee answers affirmatively to item two, discuss the nature of the information without revealing the confidential terms. The company might also consider contacting an employee's former employer if it is likely to reduce the risk of a future dispute. If the employee has existing agreements with a former employer, the company should review the agreements, unless the terms of the agreements are confidential.

All documents – electronic or physical – containing trade secrets should be clearly marked, through a uniform system for designating sensitive documents, with a legend or notice of the confidential nature of the information. This would include using "Confidential" on each page. For example:

> *This document contains trade secrets or otherwise confidential information owned by the Company. Access to and use of this information is strictly limited and controlled by the Company. This document may not be copied, distributed or otherwise disclosed except where expressly authorized by the Company.*

Being explicit, in terms of labeling documents, will help establish that the company has taken steps to keep the information confidential – a key element in proving documents contain protectable trade secrets.

Companies today must also wrestle with a smartphone-dominated reality, where nearly every employee has a computer in their pocket, complete with a camera and often access to corporate data such as email. A recent study suggested that 40 percent of employees download work files to their smartphones and tablets. As a result, BYOD policies are essential to securing confidential data.

A BYOD policy needs to begin by identifying what personal devices are and are not acceptable in the workplace. Compatibility with corporate software needs to be ensured and disclosure of the extent of IT support to be expected needs to be detailed. Limitations should be detailed regarding the download, installation and use of applications that might pose a security risk or which allow unauthorized downloads of company confidential information, including automatic storage back-ups such as iCloud.

The BYOD policy should also establish a security protocol for all personal devices, including password or screen lock mechanisms. Employees should be required to immediately report lost or stolen devices to a hotline so steps can be taken right away to prevent unauthorized access.

Companies need to clearly inform employees of their right to utilize wiping software to delete data on personal devices should these phones, tablets and computers be stolen or retained by the employee upon departure. In this process, personal, non-corporate data is often deleted. Companies can set up policies to ensure that non-corporate information is retained prior to the wiping.

Well-written employment agreements are one of the more effective ways to protect trade secrets and proprietary goodwill. These can include:

- Non-disclosure / confidentiality agreements;
- Covenants not to compete;
- Agreements not to solicit customers or other company employees;
- Agreements to return all company property upon termination; and
- Assignments of intellectual property rights.

An increasing concern in today's knowledge-driven economy is a company's right to employee created inventions and intellectual property. These assets must be protected in the form of a written agreement, often referred to as an "assignment-of-inventions". Such agreements generally provide that the company owns all intellectual property created by the employee in the course of the employee's employment.

Globally:

In the United Kingdom (Scotland, England, Wales and Northern Ireland), it is very common for employment contracts expressly to include the following "business protection" provisions:

- Confidentiality undertakings;
- Intellectual property ownership provisions;
- Restrictive covenants providing for:
    - Non-competition (prohibition from joining a competing company post-termination);
    - Non-solicitation (non-poaching of customers, clients and staff); and
    - Non-interference with suppliers
- Not identifying one's self as being connected with the departing employer post-termination; and
- Return of company property on termination of employment.

These provisions are frequently found in the service contracts of senior executives and key employees. However, in certain business sectors, such as technology, media and sales, these provisions are increasingly becoming more common – particularly for those with a front-facing customer and sales role.

Employment policy documents and handbooks also commonly contain the following provisions in the UK:

- A social media policy to address the advent of new technology and the possibility of employee data leakage through Twitter, LinkedIn and Facebook in particular;
- A BYOD policy addressing the popularity of smartphones and other tablet devices as businesses adapt to flexible working; and
- Acceptable use policies in relation to Internet use and emails.

In Luxembourg, due to a rather flexible legal framework, employers are in principle free to take any action they deem appropriate to prevent data and trade secret theft. Usually, the employment contract signed between the employer and the employee refers to internal policies which are mandatory. These policies typically refer to confidentiality rules and non-usage of insider information – except in the proper performance of the employee's duties.

Employers may also verify under certain circumstances the criminal background of new hires (e.g. by requiring a criminal record be produced prior to the beginning of the employment relationship).

In the Netherlands, employment contracts will generally contain confidentiality clauses with penalty sums. In addition, companies may use email logging systems, subject to certain terms and conditions. From an employment perspective, the Works Council will need to approve such a system. From a data protection perspective, companies should ensure that the logging is limited as much as possible to traffic data (e.g. sender, recipient, date and time). The content of emails should, in principle, only be monitored if there are reasonable grounds to suspect that an employee has misappropriated company information and then only to the extent strictly necessary within the scope of the investigation. Accordingly, any emails marked private should not be reviewed.

Companies can impose certain restrictions on use of BYOD devices and company phones as well as installing mandatory security measures on such devices. Companies are allowed to monitor workplace Internet usage by employees, but again only to the extent necessary within the scope of an investigation.

Note that in case law, employees who have been dismissed for theft of company data and trade secrets have often not been protected from dismissal even if the evidence against them seemingly proved a breach of mandatory data protection regulations. However, dismissals of such a nature have often led to increased compensation via severance packages. Companies should have policies in place for the monitoring of Internet, email and associated technologies and devices. This will give them a stronger position versus an employee in a dismissal scenario.

In Germany, preventive measures regarding employee data theft and trade secrets include:

- Employees signing that they have a duty to maintain data confidentiality and/or to exercise discretion about trade secrets;
- Trainings in data protection law;

- Policies regulating the use of employees' own electronic devices for employment purposes (BYOD policies);
- IT-security concepts (back-up-concepts, virus protection, firewall, password protection);
- Rules for data protection control, such as (1) no access for and no usage by unauthorized persons regarding data processing systems, (2) measures ensuring a documentation of who, how and when inserts, changes or deletes, personal data in data processing systems, and (3) measures ensuring protection of personal data from destruction or loss;
- Data avoidance and data economy compliance guidelines; and
- Contractual penalties in the case of trade secret theft.

In Japan, measures to prevent information leakage are examined from the aspects of physical management, technological management and human management.

Physical management includes express indications that information is secret, separate storage of sensitive information, video surveillance of data storage areas by security cameras, restrictions on removing/reproducing the media on which such information is recorded, accompanying any third-parties entering into such storage areas and similar measures.

Technological management includes the preparation of manuals and restrictions on the number of personnel with access authority. Education and training of employees and other staff, in addition to the maintenance of confidentiality by way of working regulations and contracts, is also implemented.

In the Philippines, preventive measures include: (1) not allowing employees to bring storage devices into the workplace; (2) providing for confidentiality clauses in employment contracts; (3) placing closed-caption televisions in the workplace; and (4) restricting internet access. These measures are codified in a company's security policy.

In Singapore, preventive measures regarding theft of data and/or trade secrets by employees involve the use of a combination of physical, technical and contractual barriers.

Physical barriers: simple marking of documents as "CONFIDENTIAL;" keeping sensitive documents in a safe, undisclosed location; locking files away after business hours or restricting/limiting access to areas where sensitive business documents are warehoused.

Technical barriers: employing IT to protect data/secrets stored in electronic files on computers/data servers.

Contractual barriers: generally involve the use of non-disclosure or confidentiality agreements and restrictive covenants in employment contracts. The law requires that such clauses have to be reasonable to the extent deemed necessary to protect a legitimate interest.

Confidentiality/Non-Competition Agreements

In the U.S., companies should require all employees who have access to confidential, proprietary and trade secret information to sign confidentiality or non-disclosure agreements. A company may legally require employees to sign such agreements as a condition of employment. If drafted properly, such agreements provide contractual remedies against an employee in the event of improper access or disclosure.

Since damages are in many cases difficult to prove, confidentiality agreements should, at a minimum, provide for injunctive relief should enforcement be necessary. Companies also may consider including a provision that requires the employee to pay the company's attorneys' fees and costs in bringing an enforcement action.

Non-compete agreements provide contractual means to prevent disclosure of confidential information. This is achieved by keeping a competitor from gaining access to sensitive data in possession of a former employee.

To be enforceable, most U.S. states require that non-compete agreements be reasonable in scope and duration and designed to protect a legitimate economic interests of the employer. Economic interests which have been recognized as legitimate include company goodwill and protection of confidential information.

Prior to issuing an injunction to enforce a covenant not to compete, courts normally will require that the employer demonstrate that the balance of harm weighs in its favor. If, for instance, it appears that interests the employer seeks to protect are slight, while the consequences of specific enforcement to the employee are grave, a court may not grant an injunction to enforce the restrictions.

Some states have made it difficult or even impossible to enforce employee non-compete agreements. In California, non-compete agreements are generally unenforceable pursuant to Business and Professions Code §16600. However, even California acknowledges the need to enforce certain agreements when necessary to protect trade secrets.

Variations in state law make choice-of-law and choice-of-forum provisions an important issue when drafting non-compete agreements, particularly in light of recent court decisions. For instance, the U.S. Supreme Court held in *Atlantic Marine Construction Co., Inc. v. U.S. District Court for the Western District of Texas*,[2] that contractual forum selection clauses should be enforced in all but the most exceptional cases.

Other states have made it easier for companies to rely on forum selection clauses. In Delaware, for instance, parties to a contract may include Delaware choice-of-law and venue provisions in their contracts which, under statute, [3] "shall conclusively be presumed to be a significant,

[2] 134 S. Ct. 568 (2013).
[3] 6 Del. C. § 2708.

material and reasonable relationship with this State and shall be enforced whether or not there are other relationships with th[e] State." Use of well drafted choice-of-law and choice-of-forum provisions ensures a company gets a "home court" advantage in any litigation that might arise over the enforceability of the non-compete agreements.

Globally:

In Croatia, Poland and Serbia both confidentiality and non-compete agreements are widely used. In Poland, generally employees at or above manager level sign such documents along with IT employees and outside media consultants. Serbian companies employ confidentiality and non-compete agreements both internally and between companies engaged in business.

In Denmark, companies frequently use confidentiality and non-compete agreements, if the employees have valuable knowledge that could harm the company if disclosed to a competitor.

Non-compete agreements are only enforced if they are entered into with employees holding a particularly responsible position. In addition, the covenant will not be enforced if it goes beyond what the court considers necessary to protect the employer against unfair competition, or if it unduly restricts an employee's right to seek employment in his or her field of expertise. An employer will have to pay compensation to an employee of 50 percent of salary, including all benefits during the period, where the non-competition agreement is in force.

With respect to confidentiality obligations found in contracts, the general rule is that such contracts will be enforced according to their terms unless the court decides that it is unreasonable or contrary to fair business practices to do so.

If non-compete agreements are not entered in to, it will be presumed that former employees are free to work for competing companies immediately after leaving their previous positions.

Unilateral impositions of confidentiality and non-disclosure agreements on employees who are leaving a company or retiring are possible and commonly used.

Even if non-compete or non-disclosure agreements are not imposed, former employees will, according to Danish case law, have a duty of loyalty after leaving a company, regardless of the reason for leaving (voluntary or otherwise). There is likewise an explicit prohibition in the Marketing Practices Act on the misappropriation and abuse of trade secrets obtained in the course of employment.

In Hong Kong both confidentiality and non-compete agreements are widely used. However, there is difficulty in enforcing such agreements as Hong Kong courts have tended to look unfavorably on non-compete provisions and will usually subject agreements to a very high level of scrutiny unless it can be proved that such provisions are necessary to protect the legitimate interests of the employer. The onus of proof tends to be quite high.

In New Zealand, confidentiality and non-compete agreements are both widely used. These provisions are typically contained in employment agreements, as opposed to separate agreements – except in unique situations.

An employer may protect its proprietary interests by including a restraint of trade clause in its employment agreements. A restraint of trade clause may contain prohibitions against competition, solicitation (of clients, customers and/or employees) or both. However, restraints of trade must be used carefully as the New Zealand Employment Relations Authority/Court consider them to be inherently against the public interest and will only uphold them to the extent they are considered reasonable.

In determining the "reasonableness" of restraint of trade clauses, the authority/court will consider factors such as:

(a) whether an employer has a genuine proprietary interest (such as trade secrets, confidential information, or close client or supplier relationships) which warrants protection;
(b) the scope and duration of the restraint;
(c) the geographical area of the restraint;
(d) the nature of the business;
(e) the seniority of the employee;
(f) whether any consideration has been paid to compensate for such restrictions; and
(g) the impact of the restraint on the individual (e.g. ability to earn a living).

The roles for which a non-compete clause may be appropriate are limited and include senior sales staff, senior management and any staff who have important relationships with clients or access to trade secrets or other highly confidential information. In most cases, a restraint against competition will also only be reasonable for a period of three-to-six months.

The restraint should be tailored to the individual concerned so that it is limited in duration, scope and geography to that which is absolutely necessary to protect the company's interests. In New Zealand, the Employment Relations Authority/Court may vary a restraint of trade clause, to the extent required to reasonably protect an employer's proprietary interests.

In Vietnam, the usage of confidentiality and non-compete agreements is common across industries. However, non-compete agreements are not enforceable in general as they violate the right of individuals to be gainfully employed.

Tools for Investigating Trade Theft and Tips for Prevention

In the U.S., departing employees pose one of the greatest risks to a company’s trade secrets and confidential information. A critical component to reducing this threat is taking preventative measures before an employee leaves.

Upon termination of employment, a company should immediately terminate computer access rights for an employee. In addition, the company should revoke the employee's access entry, cancel cell phone access and retrieve any company owned materials, including policy manuals, directories and equipment.

An exit interview is an effective way to remind departing employees of their post-employment obligations. A company should inform employees that all of their contractual obligations survive termination of employment, and that it expects that they will continue to comply with such obligations. It is advisable to provide employees with copies of relevant agreements. Interviewers should confirm that all proprietary information in whatever form has been returned and/or destroyed.

The exit interview also is a time to inquire about an employee's future plans, including questions about the nature of work they are expected to perform for their next employers. Departing employees should also be notified of the company's right to contact new employers with respect to existing contractual obligations. In certain circumstances, a company may want to consider contacting successor employers in order to reduce the risk that former employees will employ or reveal company trade secrets.

Most employee data theft occurs around the time of employment termination. Thus, investigations of theft should focus on this time period.

For instance:

- Did the volume of an employee's emails significantly increase, particularly emails sent outside of the company?
- Was there any change in employee work habits, either staying unusually late or arriving unusually early?
- Was there evidence that the employee made downloads to external devices, or accessed or copied an unusual amount of documents near the end of his/her employment?

All of the above issues could be signs of employee data theft that require action by an employer.

An employee's computer hard drive, mobile device and other data storage systems are potential sources of valuable evidence, but these can inadvertently be lost or compromised. Even if a former employee had "deleted" certain information, a careful analysis can reveal useful evidence that could inadvertently be overwritten and/or erased. It is imperative therefore that a company maintains the integrity of any systems that it believes may contain evidence of misappropriation.

Most investigations will require the use of someone from a company's IT department who has experience examining file fragments and user activity. In some cases, however, it will be

advisable to retain a computer forensic specialist who can assist the company in identifying potentially relevant evidence of misappropriation.

A computer forensic specialist can recreate the actions of a former employee by analyzing computer systems. This can lead to information such as whether a former employee attached an external storage drive to copy data or used an Internet-based storage account. A specialist could also look for evidence that an employee attempted to "cover their tracks" by utilizing a wiping program.

Globally:

In Luxembourg, there is no defined protocol for companies to investigate trade secrets theft. Rather, methods are defined and determined on a case-by-case basis.

As generally stipulated in employment contracts, at the moment of termination of the employment relationship, an employee is obliged to deliver to his/her former employer all company documents including copies, materials, devices and software which may be in their possession or under their control.

Besides this general provision, companies may investigate trade secret theft by organizing exit interviews, forensic examinations or any necessary action which is deemed appropriate if there are reasons to believe that an employee has stolen trade secrets and/or retained confidential data. However, these investigations must be conducted within the framework of the country's legal provisions (e.g. the right of employee to privacy).

In Bulgaria, Bulgarian Labor Law does not provide for a specific procedure for investigation of data and trade secret theft. In practice, employers craft their own policies for investigation based on the specifics of their business activity. These processes usually take place on a case-by-case basis and vary depending on the specific situation.

One of the most common tools for an employer to carry out an investigation is to receive information from counterparties and/or competitors, which may contain evidence of trade secret theft. Employers may legally collect information from a wide variety of sources to this end. Another useful tool that employers may use is to check the hardware used by the former employee. In a case where an employer wishes to impose disciplinary sanction, it should document the entire investigation procedure in formal, statutory required documents (e.g. request for explanations to the suspected employee and the other individuals that may have information; and order for imposition of disciplinary sanction, describing the facts and the collected evidence, etc.).

In Turkey, as employment contracts establish a personal relationship between the employer and the employee, the employee is under a loyalty obligation and is expected to notify the employer of any and all situations which may harm, or have the potential to harm, the welfare and the reputation of the company. A company may choose, in the course of an investigation,

to analyze emails of suspected employees while respecting the limitations of relevant laws and regulations.

If a company believes that data is likely to be misappropriated, it may opt to conduct an exit interview with the employee in question, ensuring that all data acquired from the company is deleted in an appropriate manner. Afterwards, termination procedures are to be followed in accordance with the Labour Law.

In Malaysia, forensic investigations – either conducted internally (banks for example, generally have a dedicated audit team), or by way of appointing specialist firms – are popular. It is also not uncommon for companies to utilize the services of private investigators and/or specialists in computer forensics.

In India, there are no prescribed rules in this respect, and companies across the country adopt all available means to detect and prevent data theft. If theft does occur, companies adopt both technology- and non-technology-based approaches to investigate. Technology-based solutions include forensic examination of the IT hardware and software involved. A frequently used non-technology-based approach is to conduct a disciplinary inquiry, involving interviews with various employees.

Civil and Criminal Remedies for Prosecuting Employees Who Share Data and Trade Secrets

In the U.S, agreements not to compete and confidentiality agreements provide contractual remedies against employees who steal trade secrets. Claims for breach of contract in the employment context follow the common law elements requiring: (1) mutual assent to the terms of an agreement; (2) adequate consideration, and (3) a breach of the contract's terms.[4]

Confidentiality and nondisclosure provisions are usually the easiest to enforce. Once a company produces evidence that information has been wrongfully removed, courts generally will enforce the terms of a contract and are usually sympathetic to a company's need to protect its trade secrets.

Enforcement of non-compete agreements, on the other hand, is viewed as a restraint on free trade, with some states even prohibiting their use outright. As a result, the party seeking to enforce these agreements must show that restrictions sought to be enforced are reasonable in geographic scope and temporal duration, and protect a legitimate business interest.[5] An employer's legitimate business interests may include preventing disclosure of confidential information, trade secrets, or damage to the employer's goodwill.[6]

---

[4] *Faw, Casson & Co. v. Cranston*, 375 A.2d 463, 466 (Del. Ch. 1977) ("The formal elements required in an agreement not to compete are the same as those required for a contract in general, namely, a mutual assent to the terms of the agreement by all parties and the existence of consideration.").
[5] *Hough Assocs. v. Hill*, No. 2385-N, 2007 Del. Ch. LEXIS 5, at *47–48 (Del. Ch. Jan. 17, 2007).
[6] *TriState Courier & Carriage, Inc. v. Berryman*, No. 20574-NC, 2004 Del. Ch. LEXIS 43, at *42 (Del. Ch. Apr. 15, 2004) (noting that "the goodwill of its clients and its confidential information … have long been recognized as legitimate economic interests of a former employer").

Misappropriation of trade secrets is a common law tort that has been codified by the Uniform Trade Secrets Act (UTSA). The UTSA has been adopted, with some variation, by nearly all states. It imposes a three-year statute of limitations, running from discovery of harm.

The UTSA, and its state law corollaries, prohibit the misappropriation of trade secrets. Conduct constitutes "misappropriation" when it involves the acquisition of a trade secret by: (1) improper means, or (2) "disclosure of a trade secret to another without express or implied consent." A trade secret is defined to include:

> *…information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.*

An employer's efforts to prevent information from being generally known are a key element of proof in establishing the existence of a trade secret. These efforts are frequently demonstrated by handbooks and other policies restricting access to and disclosure of confidential business information, the use of employee-specific usernames and passwords, and other similar business practices.[7]

Because the UTSA codifies common law principles, it preempts certain predecessor causes of action.[8] The statute expressly preempts conflicting tort causes of action, but preserves contractual remedies and criminal remedies generally, and other civil remedies provided that they are not premised upon a theory of misappropriation.[9]
Federal and some state statutes provide protection where an employee has used his or her employer's technology to access confidential and proprietary information in aid of unlawful competition. This category of legislation, known as "computer misuse statutes," generally stems from criminal laws that authorize civil actions.[10] These statutes, originally intended to address property crimes involving computers, have now been extended to address employee malfeasance.[11]

"While no two statutes are identical, all share the common trigger of “access without authorization” or “unauthorized access to computers,” sometimes in tandem with its close cousin, “exceeding authorized access to computers." The federal statute – the Computer Fraud

---

[7] *See*, *e.g.*, *Great Am. Opportunities, Inc. v. Cherrydale Fundraising, LLC*, 2010 Del. Ch. LEXIS 15, at *23 (Del. Ch. Jan. 29, 2010).
[8] Unif. Trade Secrets Act §7(a).
[9] *Id.* at §7(b).
[10] *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1615 (2003) ("Congress and all fifty state legislatures responded to the difficulties of prosecuting computer misuse as a property crime by enacting new computer crime statutes.").
[11] *Joseph Oat Holdings, Inc. v. RCM Digesters, Inc.*, 409 Fed. App'x 498, 506 (3d Cir. 2010) (discussing the expanding scope of the CFAA); *P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC*, 428 F.3d 504, 510 (3d Cir. 2005) (same).

and Abuse Act (CFAA) – imposes liability where an individual "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains – information from any protected computer."[12] The CFAA expressly authorizes civil actions for compensatory, equitable and injunctive relief.[13]

The term "protected computer" is defined to include any computer used in or affecting interstate commerce.[14] The term "exceeds authorized access" is defined to include an individual's access to a computer "with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[15] The term "authorized" is not defined. The CFAA also imposes a damages floor of $5,000 in one year, before jurisdiction is conferred.[16]

Because most employees have authority to access their employer's computer systems, the focus of CFAA litigation in the employment context is the scope of an employee's authority and the intent an employee has when accessing the system to obtain information. The most common defense to a CFAA claim is that an employee obtained the documents in the lawful performance of his or her duties, and only later converted the property to an allegedly improper use.[17]

Conversion is the wrongful exercise of dominion over the property of another.[18] A claim for conversion must generally arise from an independent legal duty that lies outside of the

---

[12] 18 U.S.C. §1030(a)(2)(C). There are several alternate bases for a civil claim under the CFAA, but §1030(a)(2)(C) provides the most broadly applicable basis for relief. *U.S. v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012) ("the broadest provision is subsection 1030(a)(2)(C), which makes it a crime to exceed authorized access of a computer connected to the Internet *without* any culpable intent") (emphasis in original). *See also WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 201 (4th Cir. 2012) ("Among other things, the CFAA renders liable a person who (1) `intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains … information from any protected computer,' in violation of §1030(a)(2)(C); (2) `knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value,' in violation of §1030(a)(4); or (3) `intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage[,] or … causes damage and loss,' in violation of §1030(a)(5)(B)–(C).").

[13] 18 U.S.C. §1030(g).

[14] 18 U.S.C. §1030(e)(2)(B).

[15] 18 U.S.C. §1030(e)(6).

[16] 18 U.S.C. §1030(g). *Grant Mfg. & Alloying, Inc. v. McIlvain*, No. 11-3859, 2012 U.S. App. LEXIS 20513, at *7 (3d Cir. Oct. 2, 2012) (affirming dismissal on a motion for summary judgment for failure to prove the damages element of CFAA claim); *Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 472 (S.D.N.Y. 2004) (describing the damages requirement as jurisdictional). *See also Triad Consultants, Inc. v. Wiggins*, 249 Fed. App'x 38, 40-41 (10th Cir. 2007) (citing cases, and indicating that the valuation relates to the information obtained, not any digital storage devices taken).

[17] *See*, *e.g.*, *ReMedPar, Inc. v. AllParts Med., LLC*, 683 F. Supp. 2d 605, 610 (M.D. Tenn. 2010) (granting motion to dismiss where "the crux of RMP's claims is that [employee] shared the information from RMP's computer system that he obtained while he had authorization to access and to obtain that information—in other words, that [employee] used the information he was authorized to obtain in a fashion that was adverse to RMP's interests and therefore beyond the bounds of his agency").

[18] *Kuroda v. SPJS Holdings, L.L.C.*, 971 A.2d 872, 890 (Del. Ch. 2009). *See generally* RESTATEMENT (SECOND) TORTS §§222A-242 (Conversion) (1965).

employment contract.[19] Prior to asserting a claim for conversion, the plaintiff must generally demonstrate that it demanded return of the converted property.[20] Failure to do so may be terminal to the claim.[21] Best practices therefore dictate that all termination letters demand the return of all company property in an employee's possession.

Theft of an employer's property is not enough to succeed on a claim for conversion. Like all torts, there must be some showing of damages.[22] Where a former employee takes property that, because of subsequent developments, is now worthless, there can be no recovery.[23] Where a plaintiff can prove damages, he or she is entitled to recover the full value of the converted property.[24] Alternatively, where damages and the return of property are insufficient remedies, a plaintiff may seek the equitable remedy of a constructive trust, which entitles him or her to "all profits or accretions" resulting from the conversion.[25]

By contrast, unjust enrichment may extend to those circumstances where an employee obtained compensation under wrongful circumstances, assuming there exists no other remedy.[26] "The elements of a claim of unjust enrichment are, "(1) an enrichment, (2) an impoverishment, (3) a relation between the enrichment and the impoverishment, (4) an absence of justification, and (5) the absence of a remedy provided by law.'"[27] Like a claim for conversion, the rights underlying a claim of unjust enrichment must exist independent of any contractual obligations.[28] While claims for unjust enrichment and breach of contract are

---

[19] *Kuroda v. SPJS Holdings, L.L.C.*, 971 A.2d 872, 898 (Del. Ch. 2009). ("Where, however, the plaintiff's claim arises solely from a breach of contract, the plaintiff generally must sue in contract, and not in tort. Thus, in order to assert a tort claim along with a contract claim, the plaintiff must generally allege that the defendant violated an independent legal duty, apart from the duty imposed by contract.") (internal quotations omitted).

[20] *Triton Constr. Co. v. E. Shore Elec. Servs., Inc.*, No. 3290-VCP, 2009 Del. Ch. LEXIS 88, at *78 (Del. Ch. May 18, 2009).

[21] *Id.* (noting an exception "when the alleged wrongful act amounts to a denial of the rights of the real owner").

[22] *See*, *e.g.*, *Rockwell Automation, Inc. v. Kall*, No. 526-N, 2004 Del. Ch. LEXIS 186, at *13 (Del. Ch. Dec. 15, 2004) (denying summary judgment where "there is a genuine issue of material fact with respect to what damages, if any, Rockwell has suffered as a result of Kall's retention of Rockwell's confidential documents").

[23] *See*, *e.g.*, *Empire Fin. Servs. v. Bank of N.Y.*, 900 A.2d 92, 97 (Del. 2006) (noting that, where records had been converted, there was no claim because the records "had virtually no value unless Empire was servicing the Bank's accounts. The Bank, by contrast, was expressly authorized to withdraw its accounts from Empire at any time, for any reason.").

[24] RESTATEMENT (SECOND) TORTS §221A, cmt. c (1965).

[25] *Hoover Indus., Inc. v. Chase*, No. 9276, 1988 Del. Ch. LEXIS 98, at *9–10 (Del. Ch. July 13, 1988).

[26] *Id.* at *81–84. But note that, in this case, the court rejected the plaintiff's unjust enrichment claim where plaintiff failed to prove that the defendant's receipt of salary from plaintiff and a competitor actually resulted in an impoverishment to the plaintiff.

[27] *Seibold v. Camulos Partners LP*, No. 5176-CS, 2012 Del. Ch. LEXIS 216, at *43 n.106 (Del. Ch. Sept. 17, 2012) (quoting *Nemac v. Shrader*, 991 A.2d 1120, 1130 (Del. 2010)).

[28] *Id.* at *43 ("Unjust enrichment is in essence a gap-filling remedy, which can be sought in the absence of a remedy provided by law.") (internal quotation omitted); *MCG Capital Corp. v. Maginn*, No. 4521-CC, 2010 Del. Ch. LEXIS 87, at *89 (Del. Ch. May 5, 2010) ("Courts developed unjust enrichment as a theory of recovery to remedy the absence of a formal contract.").

mutually exclusive, they may be pleaded in the alternative.[29] The remedy for unjust enrichment is disgorgement of the unjustly obtained benefits.[30]

Breach of fiduciary duty is yet another cause of action sounding in tort.[31] A claim for breach of fiduciary duty requires proof of two elements: (1) that a fiduciary duty existed and (2) that the defendant breached that duty.[32]

There are three primary duties that arise in the employment context: good faith, loyalty, and fair dealing.[33] An agent's fiduciary duties to his or her principal arise from the general proposition that "when taking action within the scope of an agency relationship, an agent's duty as a fiduciary is to act loyally for the principal's benefit." [34]A claim for breach of fiduciary duties may address a variety of competitive activity, including misuse of a principal's confidential information, solicitation of a principal's customers while still employed, conspiracy to bring about a mass resignation and use of a principal's resources to compete with the principal.[35]

Fiduciary duties apply principally to an organization's officers, directors and key managerial personnel.[36] Because these individuals are frequently subject to employment contracts, claims for breach of fiduciary duties may be foreclosed as superfluous.[37]
Remedies for a breach of fiduciary duty can vary and include equitable and monetary relief. Among the equitable relief available is an injunction or rescission of any underlying contract.[38] Where equitable relief, alone, is sought, the plaintiff need not prove damages.[39] Monetary relief includes damages resulting from the breach of duty, disgorgement of any unjust enrichment (including compensation and commissions obtained while employed by and competing with the employer) and punitive damages where permitted by established principles

---

[29] *Breakaway Solutions, Inc. v. Morgan Stanley & Co.*, No. 19522, 2004 Del. Ch. LEXIS 125, at *56 (Del. Ch. Aug. 27, 2004) ("An unjust enrichment claim is not to be dismissed because it is pled in the alternative to the breach of contract claim.").
[30] *SEC v. Hughes Capital Corp.*, 124 F.3d 449, 455 (3d Cir. 1997) ("Disgorgement is an equitable remedy designed to deprive a wrongdoer of his unjust enrichment.").
[31] *Hamilton Partners, L.P. v. Englard*, 11 A.3d 1180, 1211 (Del. Ch. 2010) (describing an action for breach of fiduciary duties as "an equitable tort").
[32] *Beard Research, Inc. v. Kates*, 8 A.3d 573, 601 (Del. Ch. 2010).
[33] Science Accessories Corp. v. Summagraphics Corp., 425 A.2d 957, 962 (Del. 1980).
[34] Restatement (Third) Agency §8.01(a) (2006).
[35] *Seibold v. Camulos Partners LP*, No. 5176-CS, 2012 Del. Ch. LEXIS 216, at *81–83 (Del. Ch. Sept. 17, 2012); *Dweck v. Nasser*, No. 1353-VCL, 2012 Del. Ch. LEXIS 7, at *50 (Del. Ch. Jan. 18, 2012).
[36] Science Accessories Corp. v. Summagraphics Corp., 425 A.2d 957, 962 (Del. 1980).
[37] Nemac v. Shrader, 991 A.2d 1120, 1130 (Del. 2010).
[38] RESTATEMENT (THIRD) AGENCY §8.01, cmt. d (2006). *See also* RESTATEMENT (SECOND) TORTS § 908(2) (1979) (regarding punitive damages).
[39] *Shocking Techs., Inc. v. Kosowsky*, No. 7164-VCN, 2012 Del. Ch. LEXIS 224, at *42 n.66 (Del. Ch. Sept. 28, 2012) ("Although damages constitute an element of the tort, a breach of the fiduciary duty of loyalty may be shown without proof of proximate damages. Here, the Court has the flexibility and the discretion that come with devising an equitable remedy and has no cause for seeking to impose a strict standard.").

of tort law.[40] In some cases courts have awarded damages based on the profits obtained by the defendant as a result of the breach.[41]

The U.S. government currently protects trade secrets through both the criminal and the public civil enforcement sections of the Economic Espionage Act of 1996 (EEA)[42]. Under the EEA, it is a felony to knowingly steal or misappropriate a trade secret to "benefit any foreign government, foreign instrumentality, or foreign agent." Section 1832 addressees the theft of trade secrets "related to or included in a product that is produced for or placed in interstate or foreign commerce." It makes it a crime to knowingly steal or misappropriate a trade secret "to the economic benefit of anyone other than the owner thereof" if the accused party "intend[s] or know[s] that the offense will . . . injure any owner of that trade secret."

The EEA applies to trade secret violations committed both domestically and outside the U.S., but it is only applicable to conduct occurring outside of the U.S. if the offender is a U.S. citizen or permanent resident alien or an organization organized under U.S. law, or if an act in furtherance of the offense was committed in the U.S. The U.S. Attorney General has the authority to bring a civil action under the EEA to obtain injunctive relief to prevent further violations, but there is no civil right to recover damages.

The Theft of Trade Secrets Clarification Act of 2012 expanded the EEA's coverage beyond products sold in interstate or foreign commerce and clarifies that the EEA also applies to trade secrets relating to products and services that a company uses internally. The Foreign and Economic Espionage Penalty Enhancement Act of 2012 increases the maximum penalties for the theft of trade secrets with an intent to benefit a foreign government or instrumentality. For organizations, the maximum fine is now $10 million or three times the value to the organization of the stolen trade secret, whichever is greater.

If the theft occurs outside the U.S., a company should consider filing a claim with the U.S. International Trade Commission (ITC). The ITC has become a popular means to combat international trade secret theft since it applies to conduct occurring outside the U.S. In order to bring a successful trade secret misappropriation case before the ITC, a company must establish that it owned a trade secret, which was misappropriated outside of the U.S., and that the articles utilizing the trade secret are being imported into the U.S. If the claim is successful, the ITC may enter an exclusion order enjoining the respondent from importing the offending articles into the U.S.

The U.S. Federal Bureau of Investigation (FBI) has made intellectual property theft a priority in its criminal investigative program. Using the EEA and other federal laws, the FBI has focused much of its resources on investigating conduct that occurs outside the U.S. involving products or services intended to be used in interstate commerce.

---

[40] Restatement (Third) Agency §8.01, cmt. d (2006).
[41] *Dweck v. Nasser*, No. 1353-VCL, 2012 Del. Ch. LEXIS 7, at *48 (Del. Ch. Jan. 18, 2012) (awarding the value of the competitor's profits).
[42] 18 U.S.C. §§ 1831-39.

The U.S. Department of Justice also has assembled a Task Force on Intellectual Property that is part of a department-wide initiative to investigate and prosecute domestic and international intellectual property crimes. The Task Force is chaired by the deputy attorney general and has pursued indictments against foreign-based companies (and their executives) for charges ranging from criminal conspiracy to trade secret theft and wire fraud.

Globally:

In Serbia, an employer may initiate lawsuit in court against a former employee who commits a violation of trade secrets. An employer may also demand:

- termination of action that might lead to the misappropriation, use or disclosure of trade secrets and illegal prohibition of acquisition, use or disclosure of information which are trade secrets;
- prevention of traffic, or confiscation and withdrawal from the market, modification or destruction of all objects that contain information that is confidential, if such data can be, directly or indirectly, available to be viewed or transferred;
- compensation of damages, including actual damages and lost profits;
- exclusion of a person as a member of the company; and
- publication of the judgment in public media at the expense of the defendant.

Criminal remedy is imprisonment of the person who illegally shares data and trade secrets.

In Switzerland, on a civil level, the remedies are action to seek compensation for damages suffered and, depending on the case, the cessation of the unlawful situation (in particular with respect to the cessation of an activity carried out in violation of a non-compete clause). On a criminal level, several provisions in the Swiss penal code and in the Law of Unfair Competition penalize the violation by the employee of data theft and trade secrets belonging to the employer. On that basis, an employer may file a criminal complaint.

In China, under Article 219 whoever commits any of the following acts of infringing on business secrets, and, thus causes heavy losses to the oblige, shall be sentenced to not more than three years of fixed-term imprisonment or detention and shall also, or shall only, be fined; if the consequences are especially serious, he or she shall be sentenced to fixed-term imprisonment of not less than three years but not more than seven years and shall also be fined:

1. obtaining an obligee's business secrets by stealing, luring, coercion or any other illegitimate means;
2. disclosing, using or allowing another to use the business secrets obtained from the obligee by the means mentioned in the preceding paragraph; or
3. violating the agreement on or against the obligee's demand for keeping business secrets, disclosing, using or allowing another person to use the business secrets he or she has.

Whoever obtains, uses or discloses another's business secrets, which he or she clearly knows or ought to know fall under the categories of the acts listed in the preceding paragraph, shall be deemed an offender who infringes on business secrets.

"Business secrets" as mentioned in this Article refers to technology information or business information which is unknown to the public, can bring about economic benefits to the obligee, is of practical use and with regard to which the obligee has adopted secret-keeping measures. "Obligee" as mentioned in this Article refers to the owner of business secrets and the person who is permitted by the owner to use the business secrets.

In China, under Article 2, whoever infringes on the civil rights and interests of others shall be liable for the tortious acts in accordance with the law.

For the purpose of the law, "civil rights and interests" shall include personal and property rights and interests such as the right to life, the right to health, rights associated with names, reputational rights, honorary rights, the right to one's image, the right to privacy, the right to marital autonomy, the right to guardianship, ownership, usufruct, security interests, copyrights, patent rights, exclusive rights to use trademarks, discovery rights, equities, right of succession, etc.

Article 10 states that an operator shall not adopt any of the following means to infringe on the business secrets of others:

1. obtaining the business secrets from right holders by theft, promise of gains, intimidation or other improper means;
2. disclosing, using or allowing others to use the business secrets of right holders obtained by the means mentioned in the preceding paragraph; and
3. disclosing, using or allowing others to use the business secrets under its possession by breaching agreements or violating the requirements of the right holders on keeping confidential the business secrets.

Where a third party obtains, uses or discloses the business secrets of others when it has, or should have, the clear knowledge of the illegal acts listed in the preceding paragraph, the third party shall be deemed to have infringed on the business secrets of others. For the purpose of this article, business secrets refer to the technical information and operational information that are not known to the public, can be used to bring economic benefits to the right holders, and have practicability and for which the right holders have taken measures to ensure confidentiality.

Article 25 of the law states that where any party infringes on business secrets in violation of the provisions of Article 10, relevant control and inspection authority shall order the same to desist from the illegal act and may, according to circumstances, impose a fine of more than CNY 10,000 but less than CNY 200,000.

In Hong Kong, civil remedies can be damages (but only to the extent the employer can prove actual loss) and injunctive relief. Criminal remedies will depend on whether the employee is prosecuted for theft.

In Japan, claim for damages may be filed against a person who has leaked information pursuant to the Civil Code, and it is also possible to claim damages and seek injunctions pursuant to the Unfair Competition Prevention Act. Also, if certain requirements are satisfied, the Unfair Competition Prevention Act provides for imprisonment for a period of not more than 10 years with labor or a fine of not more than JPY 10,000,000 or both with respect to a person who has leaked the information, and a fine of not more than JPY 300,000,000 with respect to a corporation involved in the leakage of the information.

It should be noted that discussions are being held regarding the regulation of the importing of products that have been manufactured outside of Japan using trade secrets that have been obtained without legal authority.

A Challenging Global Problem

The issue of trade secret theft will continue to be a top concern for employers for the foreseeable future. As no single strategy is a panacea, employers need to stay up-to-date on technological and legal developments and continually evolve and refine their prevention and detection protocols while understanding the civil and criminal remedies available.