Identifying and Calculating Recoverable Damages and Predicting Risks in Cyber Security Breaches

Laura Caldera Taylor, Esq., and Thomas L. Hutchinson, Esq.

Cyber security breaches often result in the improper transfer of personal identifying information, or sensitive financial and health information. This discussion focuses on the identification of potential cyber security breaches and how courts are addressing the presentation of such cases, including the issue of damages.

Introduction

Cyber security breaches are a relatively new phenomenon. As such, there is currently not a well-developed body of case law to provide a clear road map for litigants as to the types of claims an aggrieved party may bring, and against whom, when personal identifying information (PII), or sensitive financial or health information has been compromised by a cyber security breach. The developing body of law on the topic appears to focus on the issue of damages.

A common theme the courts grapple with is what claims are available to plaintiffs whose PII and sensitive data has been compromised in a cyber security breach. In conjunction with that analysis, the question of what damages are recoverable as a result of a cyber security breach arises. By way of example, courts are asked to decide whether, due to a data breach, the loss of PII or sensitive financial or health information—in the aggregate—gives rise to a claim for damages for individual plaintiffs, and if so, what are the elements of those damages (i.e., credit monitoring costs, diminution in value of goods and services, actual loss, etc.).

As demonstrated in the *Sony* case addressed below, courts have found that where there has been no showing that the data has been fraudulently used—such as by opening up a fraudulent account, making fraudulent charges, or withdrawing funds without authorization—plaintiffs cannot recover for credit monitoring services. On the other hand, where a plaintiff alleges that his or her PII was fraudulently used, a claim for actual damages may be permitted even if the fraudulent use occurs as late as 14 months after the breach.

It becomes easy to see, then, how the litigation strategies around the approach to damages become critical in the cyber security breach arena. If credit monitoring is not a measure of a plaintiff's harm, should plaintiffs monitor their credit after a cyber security breach? If plaintiffs do not monitor their credit, who bears the risk of fraudulent activity perpetrated with stolen PII or sensitive financial data? And, from a strategic perspective, is an ounce of prevention really worth a pound of cure? In that respect, did Target get it right by providing credit monitoring services to its customers rather than litigating the issue of whether credit monitoring is an element of damages?

This discussion provides an overview of the Target security breach, case studies on four data security breach cases, and an overview of the types of damages potentially available in data breach cases.

Overview of the Target Security Breach

The security breach at Target captured America's attention. While news accounts vary slightly, it

appears that between November 27 and December 15, 2013, hackers gained access to Target's computer system and obtained both credit card data for approximately 40 million Target customers, and personal identifying information (name, e-mail addresses, phone numbers, etc.) for approximately 70 million Target customers.[1,2] Interestingly, it appears that the hackers did not directly hack Target's computer systems. Instead, they gained access to Target's computers through a third-party vendor[3,4]—Fazio Mechanical Services, Inc.—"a full-service mechanical contractor that specializes in the design, installation, and service of the most advanced, cost-effective and environmentally-friendly supermarket refrigeration systems in the industry."[5]

The blogger who first broke the Target breach story reported that the breach may have been initiated some two months before any data was stolen by a malware-laced phishing e-mail sent to Fazio Mechanical employees.[6] Citing two investigating sources, that blogger indicated that the specific malware used in the Target hack was Citadel. Citadel is believed to be a password-stealing bot program derived from the ZeuS banking trojan.[7]

By way of background, malware simply means malicious code.[8] Malware operates in many ways, all of which are intended to damage a computer, disrupt an internet connection, or steal information.[9] There are many forms of malware. Viruses are a type of malware that spread/reproduce by attaching themselves to a host executable file and becoming active when a user runs or opens the infected host file or program.[10] Opening the infected host program activates the virus.[11] Typically, the host program or file keeps functioning, but sometimes a virus will mutate or destroy the host file.[12] Viruses cause anywhere from annoying damage to a computer to denial of service. They are spread when the host file or document is transferred, often in an e-mail attachment.[13]

Trojans are harmful software that appears legitimate.[14] Once loaded and executed on a computer, trojans can cause a wide range of harm, from causing annoying pop-up windows, deleting files, stealing data, activating or spreading other malware, or creating back doors to give thieves access to infected system.[15]

Bots are automated processes, often tasks or services typically performed by people, that interact with network services.[16] Bots are not isolated to malware—they are often used positively.[17] When created by computer hacks with bad intent, they can self-propagate, log key-strokes, steal passwords and financial data, relay spam, and open back doors for thieves.[18] Importantly, a bot-infected network typically is not readily detectable

To guard against malware attacks, many individuals install anti-virus software on their personal computers. The industry standard for data security for a business that accepts cardholder data is believed to be the Payment Card Industry Data Security Standard (PCI DSS).[20] The PCI DSS provides minimum standards of technical and operational standards applicable to "all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD)."[21] The PCI DSS sets out the following six primary principles:[22]

1. Build and maintain a secure network and systems
2. Protect cardholder data
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy

Within this construct, the current version PCI DSS 3.0 contains 12 specific requirements that all companies accepting cardholder data must follow including, among others, that companies: (1) encrypt transmission of cardholder data across open, public networks; (2) maintain a Vulnerability Management Program; (3) protect all systems against malware and regularly update anti-virus software or programs; and (4) develop and maintain secure systems and applications.[23]

In an online story run by *USA Today*, a cyber security expert opined that Target likely was not compliant with PCI DSS 3.0, which was scheduled to go into effect a few weeks after Target's security breach.[24] The explanation provided for this conclusion is multifaceted. First, the mere fact that the breach involved so much data and went undetected for 18 days suggests, according to the article, logs and firewalls were not monitored daily for unusual activity.[25] Second, the article opines that under PCI PSS 3.0, companies are required to identify malware threats for all platforms, not just those most likely to be attacked. That means that companies must identify threats on everything from smartphones to tablets, and computers to point of sale technology where cards are used to make purchases.[26] Third, the article points to weaknesses in the cards themselves, noting that Target had not implemented chip-and-pin technology for its cards. That said, the article concludes that the vulnerability likely existed within Target's point of sale technology, which would have rendered

moot any added security offered by chip-and-pin technology in the cards themselves.[27]

One area where Target has received considerable criticism is in its failure to act more quickly. As more becomes known about the attack, the criticism has become more intense. It has been widely reported that two weeks before its customers' credit card numbers and PII were stolen, Target received alerts about suspicious activity from FireEye,[28] the malware program Target invested some $1.6 million in six months before the attack.[29] News accounts suggest that FireEye correctly notified Target when the initial malware was installed, and subsequently when a new version of the malware was installed.[30] Unfortunately, it appears that Target did not act upon those notices.

With this background, it is not surprising that Target is facing a number of lawsuits. While the number is undoubtedly growing at a rapid pace, Business Week reported in March of this year that more than 90 lawsuits had been filed against Target.[31] Additionally, it has been reported that in response to the breach, Target had already spent $61 million by February 1.[32] And, to avoid losing customers, Target promised that consumers would not have to pay any fraudulent charges resulting from the breach.[33]

Cybersecurity Data Breach Case Studies

In re: Sony Gaming Networks and Customer Data Security Breach Litigation[34]

After several online networks available through Sony's Play Station gaming platforms were hacked and customer PII was compromised, multiple lawsuits filed across the country were ordered into multidistrict litigation in the Southern District of California. A class action complaint in the multidistrict litigation was dismissed in part principally on the issue of damages.

Among other things, the court found that the cost of credit monitoring, and diminished value of their gaming consoles, were insufficient to allege damages under their negligence claims. However, the court found that plaintiffs adequately pled claims for restitution to recover the costs of their gaming consoles under plaintiffs' California consumer protection claims. The court dismissed plaintiffs' Data Breach Act claims which sought damages for delayed notification of the breach on the basis that plaintiffs failed to adequately allege damages flowing from the delay as opposed to the breach itself.

In addition to playing games, Sony's PlayStation Portable hand-held device ("PSP") and the Play station 3 console ("PS3") allow consumers to connect to the Internet to access certain Sony online services, and the Play Station Network ("PSN").[35] Access to the Sony online services and PSN are free, but consumers can, for a fee, purchase video games, and access certain third-party services such as Netflix and MLB.TV.[36] In order to set up an account, a consumer is required to enter into a Terms of Service User Agreement, agree to Sony's Privacy Policy, and provide Sony with PII including their: name, address, e-mail address, date of birth, and credit/debit number, expiration date, and security codes.[37]

In May 2011, the *Huffington Post* reported that Sony officially acknowledged that the company had fallen victim to a criminal cyber attack at its data center in San Diego, California.[38] The *Huffington Post* showed a dramatic photo of Kazuo Hirai, chief of Sony's PlayStation unit, and two other executives with their heads bowed in the traditional style of a Japanese apology.[39] Hirai indicated that PII, including potentially data from 10 million credit cards, for its PlayStation Network customers was compromised, but the company had no direct evidence data was actually stolen.[40]

Not surprisingly, it wasn't long after Sony's executives made their public apology that a series of lawsuits were filed. By August 18, 2011, the multidistrict panel had ordered some 56 separately filed lawsuits, from California to Southern Florida, to be transferred to the District Court for the Southern District of California to proceed as coordinated or consolidated cases.[41] In the multidistrict litigation, Plaintiffs alleged that Sony's systems were hacked on April 16 or 17, 2011. Plaintiffs further alleged that Sony learned of the security breach as early as April 17 but failed to promptly notify customers choosing instead to simply take its content offline—for nearly a month—with a notice to customers that certain functions were "offline."[42] According to plaintiffs, it was not until May 2, 2011, that Sony customers first learned that their PII was at risk due to a cybersecurity breach.[43] Plaintiffs allege, citing to a CNet.com article, that Sony offered free identity theft protection to its customers for a limited and inadequate period of time.[44]

Plaintiffs in the multidistrict litigation brought a class action lawsuit asserting 51 claims which the court categorized into nine subgroups: (1) negligence, (2) negligent misrepresentation, (3) breach of express warranty, (4) breach of implied warranty, (5) unjust enrichment, (6) violation of state consumer protection statutes, (7) violation of the California Database Breach Act, (8) violation of Federal Fair Debt Reporting Act, and (9) partial

performance/breach of the covenant of good faith and fair dealing.[45] On Sony's motion to dismiss, the court addressed each category separately. The plaintiffs plead their claims under the laws of each of the jurisdictions in which one or more plaintiffs reside.

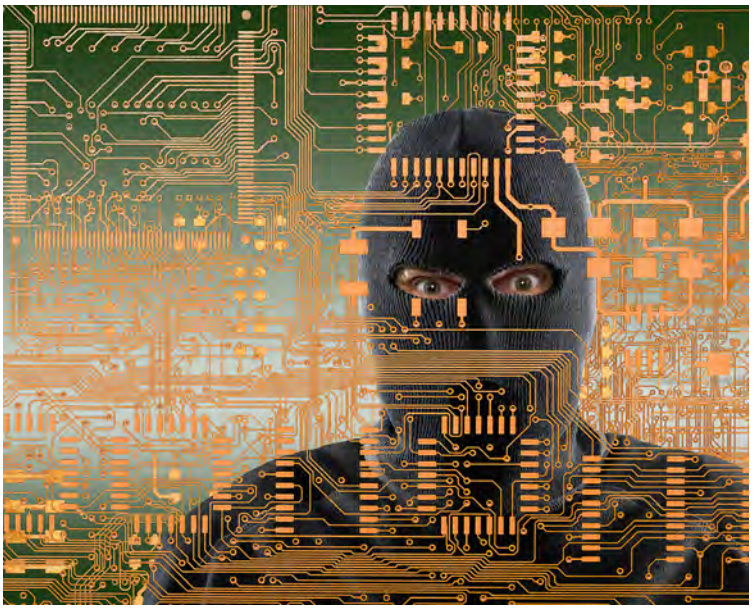
As to the negligence claims plead under the laws of Florida, Missouri, and Ohio, the court was troubled by plaintiffs' failure to plead their causation and damages theories with specificity. Instead, the court found that plaintiffs' allegations that they suffered "economic injury and property damage" as a result of the cybersecurity breach were "wholly conclusory, and therefore fail to put the court or Sony on notice of the specific relief requested."[46]

Interestingly, when analyzing plaintiffs' negligence claims under the laws of California and Massachusetts, the court noted that the factual allegations were identical to those set out in plaintiffs' Florida, Missouri and Ohio negligence claims.[47] Although the court found the allegations under the latter insufficient for failure to allege damages with specificity, the court noted that the damages alleged under the California and Massachusetts claims were "the cost to purchase credit monitoring services, loss of use and value of Sony Online Services, loss of use and value of Third Party Services, and a diminution in value of their Consoles."[48]

The court first focused on plaintiffs' allegation that Sony's delay in notifying customers of the cyber security breach gave rise to a negligence claim. On that theory, the court found that although plaintiffs alleged a brief delay, they failed to allege that their injuries were proximately caused by the alleged delay, and not the cybersecurity breach itself and dismissed those claims without leave to amend.[49]

The court went on to analyze the negligence claims directed to plaintiffs' theory that Sony owed them a duty to provide reasonable network security. As to those claims, the court first found that plaintiffs' allegations that they provided their PII to Sony, that Sony failed to employ reasonable means to protect it, including utilizing industry-standard encryption, sufficiently alleged a legal duty and corresponding breach.[50] However, the wheels again fell off plaintiffs' complaint when it came to pleading damages. Sony alleged that the damages claimed—cost of credit monitoring services, loss of use and value of Sony Online Services, loss of use and value of Third Party Services, and diminution in value of plaintiffs' consoles—were barred by the economic loss doctrine.[51]

Put differently, Sony asserted that plaintiffs did not allege personal injury or property damages. Instead, plaintiffs sought to recover purely economic losses. And, under the economic loss doctrine,



plaintiffs had to allege a special relationship in order to recover on their negligence claims.

Somewhat confusingly, the court reviewed the services agreement between Sony and the relevant plaintiffs and concluded that there was a special relationship, but that plaintiffs failed to allege "a 'special relationship with Sony beyond those envisioned in everyday consumer transactions, and therefore, negligence is the wrong legal theory on which to pursue recovery for Plaintiffs' economic losses."[52] Interestingly, the court went on to support its finding that there was no special relationship—that is, beyond the special relationship envisioned in everyday consumer transactions—by analyzing plaintiffs' claimed damages.[53]

First, the court found that plaintiffs could not recover for their alleged loss and value of the Sony online and third-party services because their losses were not proximately caused by Sony's alleged failure to provide reasonable network security and/or "did not result in a measurable loss."[54] The court explained that plaintiffs' claim to these damages was "nonsensical" in light of plaintiffs' admission that Sony owed them no duty to provide uninterrupted services—how then, the court surmised, could Sony be liable for an interruption in the services.[55]

The decision is most interesting, perhaps, with regard to the court's analysis of plaintiffs' claim for damages relating to the cost of credit monitoring service. As to those costs, the court found that plaintiffs failed to "allege why these prophylactic costs were reasonably necessary, and therefore proximately caused by Sony's alleged breach."[56] The court surveyed other data breach decisions on the issue of credit monitoring and concluded that the prevailing approach is to treat credit monitoring

similarly to medical monitoring—that is, if the state allows recovery for medical monitoring, which California does, and the plaintiff adequately alleges a threat of identity theft, a plaintiff may seek to recover credit monitoring costs.[57]

Unfortunately for plaintiffs, the court set a very high bar for pleading a "threat of identity theft." In fact, the court's opinion suggests that plaintiffs would need to allege actual identity theft such as the "opening of unauthorized accounts" in order to meet the "high burden" to prove a "threat of identity" theft in a data breach case.[58]

Finally, the court found the allegations that plaintiffs suffered damage due to a diminution in value of their consoles to be insufficient because the allegations failed to address an "appreciable, nonspeculative harm."[59] The court found this category of damages to simply consist of plaintiffs' conclusory allegations that there was a diminution in the value of their consoles without an explanation as to why—by way of example, whether plaintiffs were using their consoles less, and if so how their reduced use was tied to the breach.[60]

The court next analyzed plaintiffs' claims for negligent misrepresentation under Ohio, Missouri, Florida, Massachusetts, Michigan, New Hampshire and Texas law.[61] The court concluded that the allegations did not give rise to a claim for negligent misrepresentation under either Ohio or Missouri law and dismissed those claims with prejudice.[62] The court did find, however, that plaintiffs "sufficiently alleged actionable misrepresentation" under Florida, Massachusetts, Michigan, New Hampshire and Texas law, but failed to adequately allege how any misrepresentations were made by defendants. The court further found that plaintiffs failed to allege a pecuniary loss suffered as a result of any alleged misrepresentation. These claims were also dismissed with prejudice.[63]

The court went on to dismiss plaintiffs' breach of warranty and unjust enrichment claims for legal reasons that do not warrant discussion here. Then the court analyzed plaintiffs' consumer protection claims. Interestingly, the same factual allegations that were insufficient to allege a cognizable harm for purposes of the court's negligence rulings were sufficient to meet the injury in fact requirement for standing under the consumer protection statutes.[64] Then, in its analysis of plaintiffs' claim for restitution under the California Unfair Competition Law and the California False Advertising Law, the court held that if plaintiffs are successful on their claims, they may be able to recover all or a portion of the purchase price of their consoles as restitution because Sony financially benefitted from the sale of the consoles—sales that were made possible, plaintiffs allege, by Sony's fraudulent conduct.[65]

The court seemed to draw a distinction between the restitution damages and "actual damages" dismissing nearly all of the deceptive or unfair practices act claims where allegations of "actual damages" was a requirement, making certain carve-outs where statutory language defined loss to encompass more harm than might ordinarily be included in an actual damages analysis, at least as viewed by this court.[66]

Finally, as relevant here,[67] the court addressed plaintiffs claims under the California Data Breach Act. Like similarly enacted statutes across the country, that statute creates a civil right of action that permits injunctive relief and the recovery of attorneys' fees and economic damages.

The California Data Breach Act requires any person or business conducting business in California that uses a computerized system to access or store PII to expeditiously disclose any data breach.[68] The Data Breach Act contains two safe harbors—one permitting a business or a person to delay notification at law enforcement's request; and second the Act contains a generic 90-day safe harbor provision.[69]

Consistent with many of its earlier rulings, the court granted Sony's motion to dismiss stating that plaintiffs failed to adequately allege damages flowing from the 10-day delay in Sony's disclosure as opposed to the breach itself.[70]

Resnick v. Avmed, Inc.[71]

In a case of first impression, the Eleventh Circuit reversed the district court's dismissal of a class action complaint's claims for negligence, breach of fiduciary duty, and breach of contract even though the alleged use of the class representatives' stolen identities occurred some 10 and 14 months after the data breach. On remand, this case ultimately became what has been reported as the first court-approved data breach class action settlement case.

In *Resnick v. Avmed, Inc.*, the Eleventh Circuit considered whether a putative class action complaint brought by two class representatives properly alleged claims for relief in a complaint filed in the Southern District of Florida that had been dismissed for failure to state a cognizable injury. The complaint alleged that AvMed provided health care services in Florida and had corporate offices in Gainesville.[72]

In December 2009, two laptops were stolen containing some 1.2 million AvMed customers' (including plaintiffs') sensitive information, including protected health information, social security numbers, names, addresses, and phone numbers.[73]

The information was not secure on the laptops, which were sold to an individual with a history of dealing in stolen property.[74]

The two named plaintiffs alleged that they carefully guarded their PII.[75] Both plaintiffs had taken steps to guard their paper and digital PII.[76] Notwithstanding their efforts, both became victims of identity theft. Ten months after the AvMed laptop theft, one plaintiff's address was changed with the Post Office, Bank of America accounts were opened in that plaintiff's name, and credit cards were activated and used to make unauthorized purchases.[77] Fourteen months after the laptop theft, an account was opened at E*Trade Financial in the other plaintiff's name and was quickly overdrawn.[78]

The Eleventh Circuit first analyzed whether plaintiffs had standing to bring their claims explaining that "Whether a party claiming actual identity theft resulting from a data breach has standing to bring suit is an issue of first impression in this Circuit. Plaintiffs allege that they have become victims of identity theft and have suffered monetary damages as a result. This constitutes an injury in fact under the law."[79] Next, for standing purposes, the court analyzed whether plaintiffs injuries were "fairly traceable" to defendant's actions, and found that they were because they became victims of identity theft after their unencrypted PII was stolen from defendant's corporate offices.[80]

Next, as required by Florida law, the court analyzed whether plaintiffs properly pled that defendant's conduct was the cause of their harm under six of the seven claims alleged in the complaint: negligence, negligence per se, breach of fiduciary duty, breach of contract, breach of contract implied in fact, and breach of the implied covenant of good faith and fair dealing.[81]

The preliminary hurdle the court had to cross was the "inferential leap they ask us to make from the initial data breach to the stolen identities" of 10 and 14 months.[82] Although the District Court was not willing to make that leap, the Eleventh Circuit was willing because, "Plaintiffs allege a nexus between the two events that includes more than a coincidence of time and sequence: they allege that the sensitive information on the stolen laptop was the same sensitive information used to steal Plaintiffs' identity."[83]

Having concluded that plaintiffs adequately alleged the required element of harm, the Eleventh Circuit reversed the District Court on five of the seven claims for relief sought in the complaint, affirming only on the negligence per se and breach of the implied covenant of good faith and fair dealing claims.

After the case was remanded, it was settled for a claims made class action settlement of $3 million.[84] The settlement agreement creates a claims made settlement fund from which the following claims will be paid: "(i) Approved Identity Theft Claims, (ii) Approved Premium Overpayment Claims, (iii) Settlement Notice and Administrative Expenses, (iv) the Fee Award, and (v) incentive awards to the Class Representatives."[85] This class action settlement is reported to be the first court-approved data breach class action settlement agreement.[86]

Patco Construction Company, Inc. v. People's United Bank, d/b/a Ocean Bank[87]

A commercial banking customer whose account was hacked brought claims against the bank under, among other things, Article 4A of the Uniform Commercial Code. At issue was whether the commercial customer agreed to the bank's security procedures, and whether those procedures were reasonable. On competing cross-motions for summary judgment the district court found in favor of the bank. On appeal, the First Circuit reversed, and left open the question of whether for liability or mitigation of damages purposes a commercial customer has any obligations or responsibilities under Article 4A, even where a bank's security system is commercially unreasonable.

In *Patco Construction Company, Inc. v. People's United Bank, d/b/a/ Ocean Bank*, the First Circuit reversed the District of Maine's decision on cross-motions for summary judgment under Article 4A of the Uniform Commercial Code which governs a bank's rights, duties, and liabilities to its commercial customers regarding electronic transfers.[88]

The facts in the case were relatively straight forward. Ocean Bank authorized six apparently fraudulent withdrawals, totaling $588,851.26, from Patco Construction Company's ("Patco") account over a span of seven days in May 2009.[89] Although the thief correctly supplied Patco's customized answers to security questions, nothing else about the six transactions was consistent with Patco's use of the account. Patco used its online banking access to the account primarily to make regular weekly payroll payments—always on Fridays; always initiated from a computer at Patco's offices in Sanford, Maine; always from a single static Internet Protocol (IP) address; and always accompanied by weekly withdrawals for federal and state tax withholding as well as 401(k) contributions.[90]

The six transactions at the center of the dispute, however, were different: they weren't (or at least not all of them were) on a Friday; they were not

initiated from a computer at Patco's offices in Sanford Maine; they were not from the same IP address; and they were not accompanied by withdrawals for federal and state tax withholdings as well as 401(k) contributions.[91] "As a result, the [bank's] security system flagged these transactions as uncharacteristic, highly suspicious, and potentially fraudulent from a 'very high risk non-authenticated device.' The transactions generated unprecedentedly high risk scores ranging from 563 to 790, well above Patco's regular risk scores which ranged from 10 to 214."[92]

The bank blocked or recovered $243,406.83, leaving a residual loss to Patco of $345,444.43.[93] Patco sued the bank, seeking to hold it accountable under Article 4 of the UCC for the loss because, among other reasons, its security system was not commercially reasonable. Both parties moved for summary judgment. Although there were other issues raised by the appeal, the Article 4 arguments were the focal point of the First Circuit's analysis.

The First Circuit explained that under Article 4A of the UCC a bank receiving a payment order ordinarily bears the risk of loss for any unauthorized funds transfer.[94] However, Article 4A permits a bank to shift the loss to a customer in one of two ways. First, a bank may show that the transfer was authorized by the person identified as the sender or that person is bound by it under the law of agency.[95] The second way a bank can avoid liability is if the

> bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if:
>
> (a) The security procedure is a commercially reasonable method of providing security against unauthorized payment orders; and
>
> (b) The bank proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer. The bank is not required to follow an instruction that violates a written agreement with the customer or notice of which is not received at a time and in a manner affording the bank a reasonable opportunity to act on it before the payment order is accepted.[96]

The bank sought summary judgment arguing that Patco agreed to its security procedures, which were commercially reasonable, and the bank transferred the money in good faith. The bank's arguments were presumably premised, at least in part, on Patco's consent to the bank's "eBanking for Business Agreement" which stated that "use of the Ocean National Bank's eBanking for Business password constitutes authentication of all transactions performed by you or on your behalf." The eBanking agreement went on to state that Ocean Bank did not "assume any responsibilities" with respect to Patco's use of eBanking, that "electronic transmission of confidential business and sensitive personal information" was at Patco's risk, and that Ocean Bank was liable "only for its gross negligence, limited to six months of fees."[97]

The First Circuit analyzed the bank's security procedures and ultimately concluded that they were not reasonable. In so doing, the court was particularly focused on the bank's requirement that all electronic transactions over $1 required answers to security questions.[98] The court was concerned that requiring frequent answers to security questions created a risk that keyloggers (a form of computer malware that monitors Internet activity and records keystrokes entered on financial sites) or other malware could capture that information. This risk was further compounded by the fact that the bank did not monitor risk alerts it received. Accordingly, the bank's motion for summary judgment was denied.[99]

The First Circuit, however, left unanswered the question of whether, for liability or mitigation of damages purposes, a commercial customer has any obligations or responsibilities under Article 4A even where a bank's security system is commercially unreasonable. Although the First Circuit did not issue any rulings on the subject, it did highlight factual issues the district court could consider in its analysis such as whether Patco should have been receiving e-mail alerts from the bank and whether the fraud was caused by malware and keylogging or whether Patco shared some responsibility.

The First Circuit concluded its analysis of the issue by saying, "Article 4A does not appear to be a one-way street. Commercial customers have obligations and responsibilities as well, under at least § 4–1204."[100] That section contains a requirement requiring the customer to promptly (within 90 days) notify the bank or risk losing any interest the customer would otherwise be entitled to receive.[101]

Shames-Yeakel v. Citizens Financial Bank[102]

After a bank demanded that a couple repay funds unlawfully withdrawn from their personal home

line of credit, then transferred to their business account before being stolen, a lawsuit was filed seeking damages for negligence, breach of contract and violation of the Truth in Lending Act, Electronic Funds Act, the Fair Credit Reporting Act, and the Indiana Uniform Consumer Credit Code. Plaintiffs voluntarily withdrew their consumer credit and breach of contract claims, and the district court granted summary judgment on the Electronic Funds Transfer Act claim, granted in part the motion on the Fair Credit Reporting Act and negligence claims, but denied the motion on the Truth in Lending Act claim. As to the negligence claim, the court allowed plaintiffs' allegations of emotional and mental pain and anguish damages allegations to survive.

The facts in this case are concerning. Plaintiffs operated an accounting and booking business from their home. The accounting business had a corporate (as distinct from their personal) account with Citizens Bank.[103]

In April 2003, plaintiffs opened a $50,000 home equity line of credit with Citizens Bank. Plaintiffs took four advances on the line—all of which appeared to have been used for personal and not business reasons.[104]

On February 13, 2007, an unknown individual made an unauthorized $26,500 withdrawal on plaintiffs' home equity line of credit using plaintiffs' user name and password. What the thief did next is intriguing—instead of removing the funds directly, and immediately, the funds were transferred from the home equity line into plaintiffs' commercial account, and were ultimately removed from that account.[105] Because the funds were ultimately removed from the business account, the bank attempted to argue that the statutory claims premised on a consumer transaction should not apply. The court was not persuaded with that argument.[106]

Next, the court found that there was sufficient evidence to support a FCRA claim. This was because Citizens reported a debt (the loan balance after the funds were stolen) arising from a debt, but failed to note on the reports that the debt was the product of a theft.[107]

The last issue to be addressed in this discussion is the court's analysis of plaintiffs' negligence claim. On that claim, the court began with a careful analysis of defendant's duty, breach of that duty, and then causation. Interestingly, the district court was willing to consider emotional and mental pain and anguish as potential damages components in this case. That is because, the court opined, "A reasonable finder of fact could conclude that Plaintiffs suffered mental and emotional anguish, and that Citizens' alleged negligence in allowing the theft to occur and then violating TILA was a proximate cause of the anguish."[108]

General Damages Discussion

There are a variety of types of damages that may be available in cyber liability cases and the nature and scope of damages will be dependent upon the following:

- Types of claims being made
- The party making the claims
- The geographic location of the claims (both from the standpoint of the claimant and alleged wrongdoer)
- The location of the alleged damages
- The specific circumstances surrounding the underlying data breach or other data breach claim

". . . the vast majority of claims arise out of data breaches, which result in the transfer of individual or entity confidential financial information to unauthorized recipients."

For example, while all parties may have claims against the entity that allowed the data breach to occur, the breaching entity may have claims against vendors or subcontractors obligated to provide advisory and/or security services. Similarly, in many instances, there will be contractual and/or common law indemnity claims that could flow upstream or downstream from the breaching party.

Obviously, the type of claim being made and the location of the claim are critical issues to evaluate in the initial phase of a damage assessment. Class action claims would generally create a substantially higher damage exposure than individual claims; however, a handful of claims by credit card issuing banks could create even greater exposure for damages, as these claims would include not only the cardholder's claims, but also claims for internal investigation, reissuance of cards and payment on behalf of the cardholder for fraudulent transactions.

Furthermore, an ever increasing number of damage claims can be made under state and/or federal law. These claims include penalties and fines for failing to adequately protect a consumer's private financial information.

General Elements of Damage Claims

While there may be a number of different types of claims arising out of the broad category of "cyber

liability," the vast majority of claims arise out of data breaches, which result in the transfer of individual or entity confidential financial information to unauthorized recipients. In analyzing a typical data breach claim, the following are the typical components:[109]

1. Detection and escalation costs
   - Forensic and investigative activities
   - Assessment and audit services
   - Crisis management team
   - Communication to executive management and board of directors
2. Notification costs
   - Create contact database
   - Determine regulatory compliance requirements
   - Engagement of outside experts (including lawyers)
   - Postal expenses
   - Secondary contacts through mail or e-mail
   - Inbound communications setup
3. Post data breach costs
   - Help desk set up
   - Inbound communication
   - Special investigation
   - Remediation (including credit monitoring and victim identity protection services)
   - Legal expenses
   - Product discounts
   - Identity protection services
   - Regulatory intervention response
4. Lost business costs
   - Abnormal turnover of customers
   - Customer acquisition activities
   - Reputation loss
   - Diminished goodwill

The average total of the above itemized data breach costs are estimated to be $188 per capita in the United States for 2012.[110]

Conclusion—Target Claim Case Study for Data Breach Damages[111]

As explained in more detail above, during the holiday shopping season of 2013, Target was the victim of a significant data breach. According to a complaint filed by a number of banks issuing cards that were stolen, 40 million Target customers' personal information was stolen. This information included payment cards, customer names, credit card or debit card numbers, expiration dates, CVV codes, and PIN numbers. Target acknowledged that the information was stolen during the time period between November 27 and December 15, 2013. After initially stating that the PIN numbers had not been stolen, and after Target offered customers a 10 percent discount during the remaining holiday shopping days, Target acknowledged on December 27, 2013, that hackers had stolen PIN numbers.

In early January 2014, Target revealed for the first time that the personal information of an additional 70 million individuals had also been stolen. This information included customer names, mailing addresses, phone numbers, and e-mail addresses.

Within days of the data breach, the Secret Service, which is responsible for protecting the United States' financial infrastructure and payment systems, became aware of 255,000 to 500,000 new stolen payment cards. The Secret Service notified Target on December 15, 2013, and Target commenced an initial investigation.

The class action complaint alleged that Target agents or employees downloaded information about best practices in data security. In addition, Target's internal information indicated that an Enterprise Risk Management system would have cost less than 3 percent of the cost of the data breach, yet Target refused to implement such a system.

Assuming the average record cost per compromised customer of $188 for the Target data breach, the total resulting damages are approximately $7.5 billion. According to the complaint, the estimated costs to banks and retailers caused by the data breach could eventually exceed $18 billion. According to the Consumer Bankers Association, the member banks have spent over $172 million to reissue stolen payment cards. This amount does not include fraudulent purchases and unauthorized cash withdrawals that the banks have had to absorb (most of the stolen data is alleged to have landed in Russia).

The banks allege that the costs they will incur include the following:

1. Canceling and reissuing access devices
2. Closing deposits, transactions, share drafts, and other accounts and taking actions to stop payments and block transactions with respect to those accounts
3. Opening and reopening deposit, transaction, share draft, and other accounts

4. Refunding and adjusting cardholders to cover the cost of unauthorized transactions relating to the data breach
5. Notifying affected cardholders
6. Paying damages to affected cardholders

The claims against Target include unjust enrichment based on the allegation that Target benefited from receiving payments on transactions, has saved costs of not implementing proper data security policies, and realized increased sales related to false assurances of security. The complaint seeks refund or disgorgement from Target of wrongfully collected funds.

The class action complaint by the banks, which was eventually dismissed without prejudice, addresses issues with respect to claims against Target, but additional claims likely exist that Target could make against professionals and consulting firms advising Target with respect to security issues. For example, if Trustwave is determined to have failed to provide correct and industry standard advice to Target, Target could not only seek indemnity for all of the damages it is being asked to pay to the banks, but also could seek to recover Target's internal investigation fees, legal fees, and lost customers, as well as damage to reputation and goodwill.

This situation resulted from Target having provided access to its computer system to a heating and air conditioning contractor that provides services to Target. As demonstrated by this situation, a relatively innocent and benign situation can turn into a global multibillion dollar damage claim that will take years to unwind and resolve.

Notes:

1. Krebs on Security, the blogger who broke the Target breach wrote about the story here: http://krebsonsecurity.com/tag/fazio-mechanical-services/.
2. *USA Today*, February 24, 2014, "Target Breach Helps Usher in New World of Data Security," available at: http://www.usatoday.com/story/money/business/2014/02/22/retail-hacks-security-standards/5257919/.
3. Krebs on Security at: http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.
4. http://faziomechanical.com/Target-Breach-Statement.pdf.
5. http://faziomechanical.com.
6. http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/.
7. *Id*.
8. http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html.
9. *Id*.
10. *Id*.
11. *Id*.
12. *Id*.
13. *Id*.
14. *Id*.
15. *Id*.
16. *Id*.
17. *Id*.
18. *Id*.
19. *Id*.
20. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf.
21. *Id*.
22. *Id*.
23. *Id*.
24. http://www.usatoday.com/story/cybertruth/2013/12/23/qa-pci-rules-could-help-stymie-target-data-thieves/4179941/.
25. *Id*.
26. *Id*.
27. *Id*.
28. *Id*.
29. *Id*.
30. *Id*.
31. http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.
32. *Id*.
33. *Id*.
34. MDL No. 11md2258 AJB (MDD) (January 21, 2014) Order Granting in part and denying in part Defendants' Motion to Dismiss Plaintiffs' First Amended Consolidated Class Action Complaint.
35. *Id*. at 3.
36. *Id*.
37. *Id*.
38. http://www.huffingtonpost.com/2011/05/01/sony-apologizes-for-psn-hack-offers-free-service_n_856008.html.
39. *Id*.
40. *Id*.
41. United States Judicial Panel On Multidistrict Litigation Conditional Transfer Order (August 18, 2011) MDL No. 2258.
42. MDL No. 11md2258 AJB (MDD) (January 21, 2014) Order Granting in part and denying in part Defendants' Motion to Dismiss Plaintiffs' First Amended Consolidated Class Action Complaint, at 4.
43. *Id*. at 5.
44. *Id*.
45. *Id*. at 11.
46. *Id*. at 17.
47. *Id*. at 19.
48. *Id*.
49. *Id*. at 19–20.

50. *Id*. at 22.
51. *Id*. at 19.
52. *Id*. at 25–26.
53. *Id*. at 26–32.
54. *Id*. at 26.
55. *Id*.
56. *Id*. at 25–26.
57. *Id*. at 27.
58. *Id*.
59. *Id*. at 29.
60. *Id*.
61. *Id*. at 32–37.
62. *Id*. at 33–34.
63. *Id*. at 37.
64. *Id*. at 49–88; 52.
65. *Id*. at 60.
66. *Id*. at 49–88.
67. The court considered several other claims that are not addressed in this article.
68. *Id*. at 88–89.
69. *Id*.
70. *Id*.
71. 693 F.3d 1317 (11th Cir. 2012)
72. *Id*. at 1322.
73. *Id*.
74. *Id*.
75. *Id*.
76. *Id*.
77. *Id*.
78. *Id*.
79. *Id*. at 1323.
80. *Id*.
81. *Id*. at 1325.
82. *Id*. at 1327.
83. *Id*.
84. Resnkick v. Avmed, Inc., USDC Southern Dist. FL, Case No. 1:10-cv-24513-JLK, Document 77-1 (2014).
85. *Id*.
86. http://www.computerworld.com/s/article/9247017/Court_approves_first_of_its_kind_data_breach_settlement.
87. 684 F.3d 197 (1st Cir. 2012).
88. *Id*. at 199.
89. *Id*.
90. *Id*. at 200.
91. *Id*.
92. *Id*. at 213.
93. *Id*.
94. *Id*. at 208.
95. *Id*.
96. *Id*.
97. *Id*. at 201.
98. *Id*. at 212.
99. *Id.* at 213.
100. *Id*. at 214.
101. *Id*. at 214–215.
102. USDC N. D. Ill. Case No. 07 C 5387, Memorandum Opinion and Order (08/21/2009).
103. *Id*. at 2.
104. *Id*. at 2–3.
105. *Id*. at 3–4.
106. *Id*. at 10–11.
107. *Id*. at 15.
108. *Id*. at 21.
109. *2013 Cost of a Data Breach Study* (Traverse City, MI: Ponemon Institute, June 13, 2013).
110. *Id*.
111. The discussion below regarding the Target data breach is based on the allegations in the class action complaint filed in Trustmark National Bank and Green Bank, NA v. Target Corporation and Trustwave Holdings., Inc., USDC, Northern District of Illinois, Eastern Division, Case No. 14 CV 2069.

Laura Caldera Taylor is a trial attorney in the Portland, Oregon, office of Bullivant Houser Bailey PC. Licensed in Oregon, she represents clients in intellectual property, directors and officers liability, professional malpractice, securities fraud, and other complex business litigation. Laura's success with intellectual property clients includes patent, trademark, copyright, and trade secret litigation in state and federal courts in multiple jurisdictions. She was involved in the trial and appeal of one of the leading cases on trademark initial interest confusion on the Internet, Interstellar Starship Servs., Ltd. v. Epix, Inc., 304 F.3d 936, 941 (9th Cir. 2002). Laura's success in D&O, securities fraud, and other complex business disputes includes state and federal litigation in multiple jurisdictions, as well as arbitrations and mediations. She was involved in one of the most complex commercial bankruptcies in Oregon's history with an estimated $1.6 billion bankruptcy estate. Laura can be reached at (503) 499-4602 or laura.taylor@bullivant.com.

Thomas L. Hutchinson is an attorney in the Portland, Oregon, office of Bullivant Houser Bailey PC, where he is chairman of the firm's business and commercial litigation group. After obtaining a Bachelor of Science degree in accounting, he spent three years as a financial consultant with a top-tier CPA firm. Licensed in Oregon and Louisiana, his litigation practice focuses on advising businesses and individuals regarding a wide range of issues with an emphasis on disputes involving financial matters. Tom's areas of expertise include a full range of commercial disputes, professional liability litigation involving claims against attorneys, accountants, and financial advisors, and securities and bankruptcy-related litigation. He has tried a number of commercial cases to judgment and verdict, and has been involved in a number of matters involving broker-dealers, hedge funds, venture capital funds, and mortgage backed-securities. Tom can be reached at (503) 499-4582 or tom.hutchinson@bullivant.com.