Hacking Through Cyber Insurance

Jes Alexander

Dickey's Barbecue Restaurant, Inc.
8150 N. Central Expressway, Suite 215
Dallas, Texas 75206
972-248-9899
jalexander@dickeys.com

Table of Contents

Hacking Through Cyber Insurance[1]

[1] The author of this paper, Jes Alexander, is deputy general counsel at Dickey's Barbecue Restaurants,

In the early eighties, Hollywood depicted hackers as benevolent characters that allowed curiosity to get the better of them. For example, in WarGames, a curious teenager played by a young Matthew Broderick unwittingly stumbled into a military supercomputer, and almost triggered a nuclear war with the former U.S.S.R. At the time, the notion of a hacker doing that much harm was laughable to security experts and hackers alike.

Nobody laughs anymore about the exploits of these cyber black hats intending to steal information and to disrupt a company's operations. Upon opening a newspaper on virtually any day of the week, you will be bombarded with horror stories of yet another company falling victim to a cyber security data breach. Most often, these stories are accompanied by a headline of "largest and most costly data breach ever." As the former director of the FBI succinctly stated, "there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."[1]

What is responsible for this trend? The 21st century is not known as the information age for nothing. Combined with exponentially falling costs to store and process data, businesses of all stripes realize that information is an invaluable resource. Now, more digital information is collected and stored by companies than ever before. As a result, strict information control is vital to companies' ability to protect trade secrets, store confidential customer information, and payment information.

However, properly securing a company is like trying to keep a dam plugged that has thousands of holes. As the many potential vulnerabilities range from the hardware, the software, and human error, perfection is a nearly impossible goal even for the largest and most sophisticated companies. As recent data breaches illustrate, attackers need only a small vulnerability to infiltrate a company's system and wreak havoc.

Therefore, digital pirates possess great power to terrorize a company on many different fronts - blackmail a small business by holding its computer system hostage, post employees' confidential information on websites, steal payment information, and espionage. Unfortunately, these digital thieves turned away from Spider Man's sage advice that, "with great power, comes great responsibility."

Given these transcendent risks, a new market has arisen - cyber liability insurance. At its core, cyber liability insurance is an amalgam of first party and third party insurance expressly designed to cover typical losses faced by a company after a data breach. These covered losses include costs related to regulatory compliance, which are a major component of any cyber loss.

As data breaches affect businesses with greater cost and consequences, the need for cyber liability insurance is more crucial than ever. In fact, insurers are currently attempting to scrub away any arguable coverage from standard liability, property, or professional liability policies. For example, the drafter of the standard commercial general liability ("CGL") policy introduced restrictive data liability endorsements gutting coverage for almost any cyber-related claim.[2] Moreover, recent court decisions involving coverage for cyber risks under standard policies have not ended well for policy holders. Thus, those companies that solely rely upon standard policies do so at great peril.[3]

Unfortunately, the procurement of cyber insurance runs into two significant problems:

Inc. Prior to joining Dickey's, Mr. Alexander spent nearly a decade successfully handling high profile insurance coverage cases and civil appeals. The views reflected in this article are not necessarily the views of the author's company.

1. Massive data breaches are a relatively new phenomena. As a result, case law is scarce and courts are currently struggling to define the parameters of liability faced by a breached company. Currently, the trend is to allow increasingly creative claims to be filed against a company after a data breach; and

2. The cyber insurance market is relatively new, and no standard policy form exists. Thus, the risks covered under cyber liability policies often vary amongst insurers. Moreover, like D&O and E&O polices, cyber policies vary by the particular insured's industry.

Thus, the coverage afforded under a manuscript cyber policy must be compared to the individual risks faced by a particular company.

Although the risks faced from company to company will vary, recent data breaches involving Sony, Target, and Anthem health insurance illustrate many of the unintuitive risks shared by all companies, regardless of size. Likewise, these three digital canaries in a coal mine highlight some of the major areas that should be addressed in a cyber policy.

I. Like Father, Not Like Sony

In the past, making a satirical movie lampooning a dictator came with little risk. Perhaps a strongly worded denunciation by the offended country, which comes with the side-benefit of free advertising for the movie. For example, the film "Team America: World Police" depicted the then-leader of North Korea, Kim Jong Il, as an outlandish and petulant villain. Eventually, he is impaled on a spiked German helmet (although he did not die, he morphs into an alien cockroach). The North Korean leader's only response was to ask the Czech Republic to ban the film – a request that was swiftly rejected.

So when Sony Pictures Entertainment ("Sony") decided to greenlight a comedy involving a similar plot-line involving the assassination of current North Korean dictator, Kim Jong-un, it is doubtful that Sony's risk managers even batted an eyelash. Unfortunately for Sony, the axiom "like father, like son" did not hold true with regard to the movie "The Interview."

In the most destructive data breach in history (for now), this electronic Pearl Harbor has left Sony debilitated. The aim of the data breach was not only to steal data, but to send a clear message to Sony. And, send a message they did.

First, Sony's crown jewels – unreleased films – were uploaded online by the perpetrators of the breach to be downloaded freely by all. Next came the release of confidential and highly embarrassing emails from executives and employees, including an email exchange calling Angelina Jolie a "spoiled brat."[4] In addition, confidential information was released of over 47,000 former employees, including some social security numbers and medical information. As a result of this breach, Sony has been forced to suspend its current film projects.

Unlike the simplistic data breaches involving Target or The Home Depot, security experts describe the Sony attack as "unprecedented in nature."[5] The techniques used were "undetectable by industry standard antivirus software."[6] Before analyzing the legal pain that is just beginning for Sony, it is significant to understand how this slow-moving disaster began.

A. "I'm Gonna Make Him An Offer He Can't Refuse"– Coverage For Digital Extortions

Three days prior to the initial wave of destruction that has gripped Sony, two Sony executives received the following cryptic and hilariously translated ransom demand:

> We've got great damage by Sony Pictures. **The compensation for it, monetary compensation we want.**

> Pay the damage, or Sony Pictures will be bombarded as a whole.
> You know us very well. We never wait long.
> You'd better behave wisely.
> From God'sApstls[7]

It is unclear whether Sony's executives thought that this hilariously-worded message was a serious demand or ever tendered it to Sony's cyber liability insurer.

Sony is just one of many companies targeted for cyber extortion. The acceleration of this cyber extortion trend is caused partially by the rise of readily available software programs digital thieves use to lock companies out from their own data, such as CryptoLocker.[8] With this readily available software, a ransom-oriented cyber thief "can take in $30 million in only a few months" according to cyber security experts.[9] As a result, cyber ransoms are not limited to large companies like Sony – small businesses are now falling victim to cyber ransoms at an alarming rate.[10]

Imagine showing up for work at your law firm on Monday morning. Instead of being confronted by the familiar Windows desktop on your computer, an ominous message greets you demanding $20,000 or the deletion of all of your firm's electronic files. Moreover, the extortionists make it impossible to access any of the files on your system, or to send emails to anyone other than the perpetrator of the cyber threat. Now imagine the amount of money that would be lost related to the business interruption and ethical quandaries that would follow if this ransom demand was ignored like it was with Sony. Would you subject your firm to such a risk on the prayer that it was a giant bluff?

Fortunately, a number of cyber liability policies provide cyber extortion coverage via endorsements. For example, one cyber liability provides coverage for "Cyber Extortion Loss … incurred by the Insured Organization as a direct result of an Extortion Threat first made against the Insured Organization during the Policy Period …"[11] Moreover, given the time sensitive nature of these cyber extortion situations, cyber policies require that ransom demands are immediately reported to the insurer. Typically, the insurer will have a special extortion-related phone number to provide notice.

The question of late notice may prove to be very interesting in future cyber coverage litigation. Will insurers that receive notice of the extortion demand only after a payment is made by an insured be successful in establishing that that they were sufficiently prejudiced by late notice to avoid coverage? For example, a shareholder at a law firm might receive an extortion demand threatening the destruction of all of the firm's electronic files within 24 hours unless $10,000 is wired to a bank account. The shareholder ignores the demand because it is badly worded and he is two days into a month long trial. The next day, the cyber extortionist makes good on his threat, and deletes all of the firm's data. Absent any late notice argument, the resulting damages of $60,000 would normally be covered under the cyber liability policy. Can the insurer assert that it was materially prejudiced by the law firm's late notice? After all, had the $10,000 extortion demand been paid, the law firm would not have suffered $60,000 in subsequent losses. Given the rise in data breaches, the answer to this question may come sooner rather than later.

B. Sony, Interrupted – Business Interruption Coverage For Data Breaches

Sony's main loss will ultimately be the business interruption that it suffered. The cyber attack has crippled Sony, disrupting all of the company's operations. For example, Sony halted the filming of movies – its bread and butter – because they could not pay vendors due to the compromised nature of its computer systems.[12] The breach has left Sony as a movie company that cannot film movies.

The business interruption coverage found in property policies typically excludes interruptions caused by cyber thieves. Enter cyber liability coverage. A typical cyber policy provides first party coverage to cover business interruptions losses (*i.e.*, net profit) caused by a cyber breach under a separate insuring agreement. Cyber business interruption coverage reimburses the insured, to the particular limits in that insuring agreement, for its business losses until the company's computer systems are restored (or would have been restored if the insured had exercised due diligence). And, like other business interruption coverages, cyber business interruption coverage does not reimburse the insured for losses related to "unfavorable business conditions, loss of market or any other consequential loss; or costs or expenses."[13]

Business interruption coverage is not just for large companies like Sony. Small companies have small or non-existent cash reserves to weather a long period with its operations shut down due to a data breach. Thus, cyber business interruption coverage may be even more vital to small companies than it is to a large company such as Sony.

C. The Employee Strikes Back (And First)

Although there is no telling if Sony would have suffered the harm that eventually befell had the ransom been paid, Sony has already been sued as a result of the breach. The breach exposed the confidential information of a huge number of employees and ex-employees, including social security numbers. After receiving notification from Sony regarding the breach, a number of ex-employees filed a class action lawsuit against Sony, faulting its lax security practices and inadequate notifications.

These types of lawsuits will typically be covered by the privacy liability portion of a cyber liability policy. With regard to the breach notifications that Sony has been required to send its employees and ex-employees that have had their personal identifiable information stolen, these expenses are covered by the privacy services insuring agreement found in typical cyber policies. Data notifications are one of the main driver of costs in cyber losses, and particular attention must be paid to insuring for these losses. Data notifications will be further explored in the proceeding section regarding retailers.

D. Not War Of The Worlds

Further, the breach raises questions of terrorism. Although denying official blame, the American government indicates that North Korea ordered the attack.[14] In fact, the United States announced further sanctions against North Korea. Although the President of the United States stated that the data breach was not an act of war, he stated that it could land North Korea back on the administration's terror list.[15] North Korea railed against the new sanctions and referred to the United States as an "inveterate repugnancy."[16]

Unfortunately, cyber liability policies are written like most other liability policies to exclude coverage for acts of war. More importantly, cyber liability policies are not uniform and require extra scrutiny to determine the precise wording of the insured's particular exclusion for war. For example, a policy's exclusion may only preclude coverage for declared acts of war. If this narrow exclusionary language is found in Sony's cyber liability policy, coverage would still exist because the United States did not classify North Korea's alleged actions as acts of war.

However, broader exclusions may exclude coverage for a much larger category of foreign aggressions than official declared wars. For example, some cyber liability polices exclude losses arising out of "acts of foreign enemies, [or] hostilities (whether war be declared or not)."[17] If this exclusion were

present in Sony's $60 million cyber liability policy, it would have been an uphill argument to avoid this broader exclusion. Therefore, it is crucially important for companies to evaluate their potential exposure to cyber terrorism when obtaining cyber coverage.

It appears that Sony chose its cyber policy wisely, and deleted or modified a broad war exclusion. Indeed, Sony's chief executive stated that "the costs from the devastating cyber attack on the Hollywood studio will be *completely covered* by insurance and will not lead to further cost-cutting."[18]

II. An Easy Target - Why Companies Accepting Payment Cards Are Major Targets

What do restaurants like P.F. Chang's and Jimmy John's have in common with retailers like Target, Michaels, Neiman Marcus, and Staples? No, they are not hoping to create the newest taste sensation of a General Tso's chicken sub-sandwich sold exclusively at these fine retail establishments. Instead, each of these retailers recently suffered massive payment card breaches.

The loot obtained by these breaches is a virtual goldmine - a trove of payment card information. Using stolen payment card information, thieves can quickly make fraudulent charges. Payment-card thieves are creative when earning an ill-gotten buck, as underground markets exist to buy and sell stolen payment card data.

Theft of customer information, such as names and addresses, may be equally valuable to some digital pirates. Customer information can be used to commit identity theft and forgery. Moreover, the wholesale theft of customers' email addresses allow thieves to create highly convincing phony emails designed to obtain sensitive personal information, such as an email that appear to be sent from your own bank.

The trend of retailer-related data breaches began in anything but earnest when T.J. Maxx was breached in 2005. At least 45 million credit and debit card numbers were stolen during an 18-month period.[19] The breach resulted from an intrusion into the company's wireless network due to its use of a relatively insecure form of encryption.[20] The breach resulted in a loss of about a quarter of a billion dollars. At the time, this was the largest retail data breach.

Even ignominious records are meant to be broken. The 2013 Target data breach compromised 40 million credit card numbers in about three weeks, and the information of over 70 million customers.[21] The source? Thieves stole the network password from a third-party HVAC subcontractor working at a few Target locations.[22] The three-week breach resulted in losses exceeding $148 million, with costs still rising today.[23]

In 2014, The Home Depot also fell victim to a data breach that exposed 56 million credit card accounts and 53 million customer email addresses.[24] The digital thieves breached The Home Depot's security in the same manner as Target – by targeting a small outside vendor that was in possession of The Home Depot's network passwords.[25] Although final figures will not be known for some time, The Home Depot lost approximately $43 million in one fiscal quarter.[26]

While data breaches involving massive retailers grab all the headlines, smaller companies are increasingly targeted because they have less sophisticated security safeguards. Most small business do not have an in-house security team or the resources to hire an outside vendor. For example, Mel's Diner in Louisiana used weak password protection in its network that resulted in the theft of nearly 700 credit cards.[27] The cost was over $50,000, a sum that would likely bankrupt a small business without proper cyber liability insurance.

Additionally, these data breaches are not limited to traditional retail stores, such as Target, or small mom-and-pop restaurants. Any company that accepts payments via credit card or that digitally stores client data - such as law firms - is a target.

Thus, the universe of companies that are at risk for suffering a data breach is vast.

What accounts for these eye-popping sums incurred by companies after a breach? A portion of this number is based upon a loss in sales due to the erosion of customer goodwill. Target's profits suffered mightily after its massive data breach during the holiday season. However, the lion's share of these huge sums lost by companies is due to the liability faced post-breach. Businesses face liability exposure on all fronts: the government, financial institutions, and customers – the absolute three worst enemies for any company attempting to make a profit.

A. The Regulators Mount Up With Costly Notification Requirements & Penalties

1. You Have Mail – Notification Requirements After A Breach

Maybe the initial data breach is a headache, but the nightmare truly begins when the regulators show up. One of the more onerous liabilities faced by a breached company are data notification laws, which are currently found in 47 states.[28] Common among these notification laws is the requirement that companies notify all individuals if any personal identifiable information is lost, stolen, or compromised.[29] For example, Texas' Identity Theft Enforcement and Protection Act statute mandates:

> Breach Notification Requirement: Any person or business that owns or licenses computerized data that includes [personal identifiable information] shall, upon a discovery of a breach, notify any resident of [Texas] whose [personal identifiable information] may be included in the breach.[30]

The costs to comply with consumer-notification laws can be staggering. Notification costs typically vary based on the number of records involved in a data breach. These expenses can range from approximately $.50 to $5.00 per individual notice.[31] Therefore, businesses must ensure that their cyber liability policies include coverage for the full range of costs in the event of a breach.

Fortunately, most cyber liability policies on the market today provide coverage for costs related to notification laws in the form of "privacy" liability coverage.[32] This form of coverage typically insures against the unauthorized disclosure of personal identifiable information. Significantly, the privacy-related portions of cyber liability policy provide coverage even where ***no*** computer-related data breach is involved.

Moreover, privacy liability coverage is typically paired with a secondary "privacy breach response services" insuring agreement that provides for a whole ranges of ancillary coverages. This coverage protects insureds from potentially ruinous expenses required by these virtually omnipresent breach notification requirements.

- **Practice Tip:** The devil is in the details with regard to notification. For example, many cyber liability polices contain a maximum number of notifications that are covered. Depending on its potential exposure, an insured can elect to purchase 1,000 notifications or millions of notifications. Thus, when purchasing a cyber liability policy, it is important to forecast the worst-case scenario for the necessary number of notifications. As data breaches often go undetected for long periods of time, the more notifications covered, the merrier.

  Equally as important are the other expenses that a breached insured will immediately face in complying with data notification laws. These costs typically include a forensics investigation to determine the extent of the breach, along with certification

from computer experts confirming that the system is secure.

Furthermore, data breaches may severely damage the company's brand. For example, Target's sales plummeted when news of its breach became public. In an effort to minimize damage to customer goodwill and preserve the brand, many companies will incur significant costs by engaging crisis management and public relations firms. And, although not required, companies typically provide additional services to affected individuals, such as call centers and identity monitoring services. Many cyber liability policies provide coverage for these expenses under separate insuring agreements. Significantly, these ancillary costs often erode the policy's aggregate limits, and thus, such costs must be carefully monitored.

2. Post Breach, All Is Not Fine

In addition to the costs associated with notifying affected consumers, many breach notification laws also allow states to impose penalties and recover damages. For example, should a business ignore the requirements to report a breach to the state under data notification statutes, the hammer will be dropped.[33] For example, Texas law penalizes companies $100 per individual per day of failed or delayed notification, up to $250,000 for a single breach.[34] Fortunately, cyber liability policies provide coverage designed for an insured's "failure to timely disclose an incident described … in violation of any Breach Notice Law."[35]

- **Practice Tip:** This coverage is typically subject to its own independent sublimit amount. Care must be taken to ensure that the sublimit amount is adequate.

In addition, penalties are often levied against companies for the data breach itself. Texas' Identity Theft Enforcement and Protection Act authorizes the Attorney General to bring an action against a company seeking "a civil penalty of at least $2,000 but not more than $50,000 for each violation."[36] Other states impose similar fines.

On the federal level, no statute expressly regulates corporate data security practices of businesses with regard to data breaches. Despite this void, the Federal Trade Commission ("FTC") asserts that it is authorized to fine companies after a data breach. To support its power to issue penalties against companies, the FTC relies upon an archaic law dating from 1914 that was designed to protect consumers from companies that engage in "unfair or deceptive acts or practices in or affecting commerce."[37] These penalties can exceed hundreds of thousands of dollars.[38]

Cognizant of civil penalties faced by companies after a data breach, cyber liability policies have evolved to provide coverage for regulatory penalties. For example, the Beazley Cyber Policy contains a separate insuring agreement subject to a specific sublimit amount for claims and expenses related to regulatory proceedings.[39] As the coverage for regulatory penalties is subject to a sublimit amount, it is necessary for the insured to determine whether the penalty sublimit is adequate.

Moreover, it is an open question in many jurisdictions whether penalties are insurable under the particular state's public policy.[40] Although Texas courts have not addressed whether civil penalties for a data breach are insurable, the Supreme Court of Texas' *Stephens Martin* decision is instructive.[41] There, the Court found it was not against public policy to allow coverage for punitive damages, which are similar in nature to civil penalties. The Court found punitive damages insurable because a company was being sued for the conduct of its employees, and the company's upper management was unaware of its employee's wrongful acts.[42] However, the Court strongly indicated that punitive damages based "extreme circumstances," such as intentional misconduct, would not be insurable.[43]

Due to the similarities between civil penalties and punitive damages, it is likely that a

similar *Stephens Martin* analysis would be applied to whether civil penalties for data breaches are insurable under Texas' public policy. Where a company negligently or unintentionally failed to prevent a data breach based on its employees' wrongful acts, coverage would likely exist for civil penalties. However, where a business acted willfully or intentionally relating to a data breach, coverage for civil penalties may not be owed for these "extreme circumstances." In fact, coverage litigation involving whether civil penalties under the Telephone Consumer Protection Act[44] for unsolicited telemarketing calls or faxes reflect the same dichotomy – penalties for negligent and unintentional conduct are insurable, but penalties for malicious conduct (triggering treble damages) are uninsurable under the particular state's public policy.[45]

B. The Game Is Rigged - The Banks Always Win

1. Merchant Services Agreements

Claims from financial institutions present another serious liability for any businesses accepting payment cards, such as retailers, medical providers, or law firms. These companies must enter into "merchant services agreements" with acquiring banks. In turn, acquiring banks maintain separate contracts with payment card companies, such as MasterCard and Visa.

To protect payment card data from digital theft, merchant services agreements typically require companies to implement strict security measures. These security measures are known as the PCI Data Security Standards ("PCI-DSS"), and were developed by the five major payment card companies.[46] The PCI-DSS standards include 12 main requirements for security management and procedures that the company must implement. [47]

Significantly, the standard merchant services agreement also mandates that businesses pay fines and indemnify the acquiring bank when a data breach occurs. These fines stem from the fact that payment card companies may penalize an acquiring bank $5,000 to $100,000 per month for PCI compliance violations.[48] In turn, acquiring banks will pass any penalties downstream to the non-compliant merchant.

Thus, it is important to evaluate whether the victimized company's cyber liability policy provides coverage for the acquiring bank's indemnification claim. For example, many cyber liability policies, such as the Beazley policy, expressly provide coverage to the insured "for PCI Fines and Costs." This coverage for PCI penalties is typically subject to a separate sublimit of liability.

Furthermore, merchant services agreements typically impose a host of additional requirements on businesses in the event of a breach. Specifically, businesses are required to determine the cause of the breach by hiring a forensics investigator, and to minimize the likelihood of a future breach. Complying with these additional requirements does not come cheap. Fortunately, many cyber liability policies cover these steep additional costs under the insuring agreement for "privacy breach response services." In particular, a cyber liability policy might cover the costs incurred:

- "for a PCI Forensic Investigator that is approved by the PCI Security Standards Council and is retained by the Insured Organization in order to comply with the terms of a Merchant Services Agreement to investigate the existence and extent of an actual or suspected compromise of credit card data;"
- "for a computer security expert to demonstrate the Insured's ability to prevent a future electronic data breach as required by a Merchant Services Agreement;" and
- "for fees charged by an attorney … to advise the Insured Organization in responding to credit card system operating regulation requirements for any actual or suspected compromise

> of credit card data that is required to be reported to the Insured Organization's merchant bank under the terms of a Merchant Services Agreement."[49]

Moreover, companies must scrutinize any contractual liability exclusions that could exclude coverage for these contractual PCI penalties found in merchant agreements. Although most cyber liability policies have some form of contractual liability exclusion, cyber policies designed for retailers typically have an exception for PCI-related penalties.[50]

2. Issuing Banks & The Unsettling Trend For Companies

Liability to financial institutions may not end with acquiring banks. Individual cardholders, like you and me, receive payment cards from financial institutions (an "issuing bank") that have a relationship with payment card companies, such as MasterCard or Visa. For example, consumers apply to an issuing bank for a credit card, such as Chase for their Southwest Visa credit card or, if you are George Clooney, the invite-only "Black Card" issued by American Express.[51]

Significantly, *no* direct relationship exists between merchants, like Target, and issuing banks, like Chase or Citibank. However, issuing banks suffer great expense after a business is breached. When a data breach occurs at a company that processes payment cards, issuing banks must cancel accounts, deal with fraudulent charges, and reissue cards. The administrative costs alone in replacing a card average $10 to $22 per card – this does not include cost for fraudulent charges that result.[52] This $22 per-card sum can rapidly get out of hand when a data breach involves the exposure of millions of credit cards. For example, it is estimated that issuing banks will incur about $400 million dollars in administrative expenses related to the Target data breach.[53]

Since no contract exists between the issuing bank and the breached company, issuing banks are often left holding the bag for these huge expenses. Issuing banks are not known as wallflowers with respect to litigation, and many are attempting to forge new precedents to hold businesses liable for these costs. In fact, litigation involving Target has given issuing banks new hope that the costs of data breaches can be passed on to the negligent business.

Specifically, after Target was breached, a group of issuing banks initiated a class action lawsuit.[54] The issuing banks allege that Target's negligent acts and omissions resulted in the data breach. In a standard tactic that has been largely successful in most data breach litigation involving issuing banks, Target moved to dismiss the class action lawsuit's negligence claim. Target's dismissal motion pointed to the lack of a contractual relationship with the banks, and argued that Target "had no duty to [the issuing banks] because there is no special relationship … and in any event, 'a person has no duty under [state] law to protect another from the harmful conduct, including criminal conduct, of a third person.'"[55] Surprising many, the federal district court rejected Target's no-duty argument, and held:

> Although the third-party hackers' activities caused harm, Target played a key role in allowing the harm to occur. Indeed, Plaintiffs' allegation that Target purposely disabled one of the security features that would have prevented the harm is itself sufficient to plead

> a direct negligence case: Plaintiffs allege that Target's "own conduct create[d] a foreseeable risk of injury to a foreseeable plaintiff."[56]

Thus, issuing banks have a new precedent in their arsenal in the form of pure negligence claims against companies for employing lax security systems. Breached companies now have another massive headache to worry about.

The mere survival of the motion to dismiss has already reaped great dividends. For the issuing banks. With regards to the Visa issuing banks, Target paid $67 million.[57] Similarly, MasterCard issuing banks really mastered the moment, as they settled for $39 million with Target.[58] Thus, a total of over $100 million was paid out by Target to the issuing banks.

This decision by the issuing banks to oppose the settlement appears prescient. On September 15, 2015, the district court certified as a class "[a]ll entities in the United States and its Territories that issued payment cards compromised in the payment card data breach that was publicly disclosed by Target on December 19, 2013."[59] Tar get has appealed the class certification to the Eighth Circuit. Regardless of the result, the issuing banks will likely receive a huge payout stemming from this breach – a result that will encourage issuing banks to take similar tactics in future breaches.

Moreover, issuing banks are also lobbying Congress to pass federal legislation that would statutorily hold companies liable for negligent breaches.[60] In fact, some states, such as Minnesota, have already passed legislation making the security standard PCI-DSS a statutory requirement where the failure to comply would result in liability to the company.[61] Texas came very close to passing a similar statute, but the proposed legislation ultimately failed.[62]

Fortunately, the emerging class action lawsuits are typically covered under the privacy liability portion of the cyber liability policy. In particular, a common privacy liability insuring agreement provides:

> [Insurer agrees to] pay on behalf of the Insured [Damages and Claims Expenses for]:
>
> theft, loss, or Unauthorized Disclosure of Personally Identifiable Non-Public Information or Third Party Corporate Information that is in the care, custody or control of the Insured Organization, or a third party for whose theft, loss or Unauthorized Disclosure of Personally Identifiable Non-Public Information or Third Party Corporate Information the Insured Organization is legally liable.[63]

Given this high potential of contagion regarding the *Target* decision, the significant legal costs dealing with class action lawsuits by issuing banks attempting to recoup their damages must be accounted for when determining the adequacy of a cyber liability policy's limits. Old damage models for cyber liability claims no longer will suffice, as they do not include losses relating to issuing banks. As the bulls-eye on companies' backs just got bigger, limits of cyber liability policy should be adjusted upwards.

- **Practice Tip:** Watch out for sublimits relating to payments made to these credit card brands (Visa, MasterCard, etc.)

pursuant to a merchant services agreement. Sublimits – which essentially function as exclusions by another names – limit coverage to a lesser amount stated in the declarations. For example, although the policy might cover third-party liabilities up to $2 million, a sublimit might existed that reduces coverage for payments related to merchant services agreements to $500,000.

3. Companies Are Clapping That Consumers May Not Have Much Of A Leg To Stand On

Not to be left out, consumers also target businesses after a breach. Consumers often file class action lawsuits against businesses asserting claims of negligence, breach of warranty, and unfair or deceptive trade practices. To date, a big impediment to these consumer lawsuits has been the fact that the financial institutions (the issuing banks and acquiring banks) bear the brunt of the blame. The issuing banks absorb the costs of fraudulent charges and administrative costs to reissue payment cards, not the consumers. Accordingly, most of the complaints brought by consumers involve the threat of future harm, such as consumers' fear that they will suffer future identity theft. Thus, the major issue is typically whether the consumer has suffered a legally cognizable injury that will support standing to bring suit - an issue that can be immediately addressed via a 12(b)(6) motion to dismiss in federal courts.

To date, both the First and Third Circuits hold that standing is lacking based on the consumers generalized notion of a threat of future identity theft or fraudulent charges.[64] The Seventh and Ninth Circuits stand on the opposite side of this debate, as they find standing for consumers to proceed with lawsuits despite any actual loss.[65] However, the Seventh and Ninth's Circuits' broad interpretation of standing may not stand the test of time based on a recent Supreme Court decision, *Clapper v. Amnesty International USA*.[66]

Clapper involved human rights organization and media groups challenging the Foreign Intelligence Surveillance Act's authority regarding wiretaps on intelligence targets. In a 5-4 decision, the Court found no standing for these groups despite their fears of imminent harm in being subject to a wiretap. Relevant to these consumer claims in a cyber liability context, the Court found that, although the plaintiffs' concerns were not "fanciful, paranoid, or otherwise unreasonable," the harm complained about was not "certainly impending." Moreover, the court held standing cannot be created "merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[67] Indeed, all but a few courts have dismissed data breach lawsuits in early stages of litigation based on the *Clappers'* apparent narrowing of standing.[68]

Nonetheless, where consumers can establish that they have been injured, standing will likely not be an impediment. For example, a proposed class action filed by 114 consumers with regard to the Target data breach has been allowed to proceed despite Target's argument that they did not have *enough* standing to establish injury.[69] However, the consumers alleged injuries for unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges. Target's argued that it was unclear from the face of

the consumers' complaints whether the expenses were reimbursed by the issuing banks. In rejecting Target's argument, the federal district court in Minnesota held that the consumers' "allegations plausibly allege that they suffered injuries that are 'fairly traceable' to Target's conduct."[70]

Like with the issuing banks survival of the preliminary motion to dismiss filed by Target, a settlement of $10 million has been reached in the Target litigation.[71] Also, Target is required to adopt heightened security measures under the settlement.[72]

Given that the consumers' main claim that survived dismissal is a plain-vanilla negligence claim under Minnesota law – a negligence standard that is virtually the same in all other states – expect even more lawsuits brought by consumers in the future. Savvy plaintiffs' attorneys will likely follow the rationale of the decision by the Minnesota court in *Target*, and bring lawsuits alleging actual damages sufficient to establish standing to bring suit. Therefore, defense costs will be an ever-increasing issue that must be considered in a cyber liability policy.

- **Practice Tip:** Unlike CGL polices where the payment of defense costs by the insurer does not decrease the amount of indemnity dollars available, cyber liability policies are typically "wasting" or "cannibalizing" polices. Each dollar paid for defense costs erodes the available indemnity limits. Thus, if an insurer that issued a $1 million cyber liability policy pays $250,000 in defense, the policy is eroded such that only $750,000 remains to pay out any judgments or settlements. When determining the amount of cyber liability coverage that should be purchased, an insured must take into account defense costs for the highly specialized attorneys that may be necessary in the event of a breach.

4. Passing The Buck – Who Can Companies Target?

The breach involving Target and The Home Depot arose from a common source – their vendors' negligence. Accordingly, companies must proactively ensure that vendor contracts provide protection in the event of a data breach. Companies should adopt an approach similar to what is standard in the construction industry. Specifically, a belt-and-suspender approach of additional insured coverage *and* contractual indemnification for data breach claims should become standard language in vendor contracts.

The requirement of a vendor to add a hiring company as an additional insured under its cyber liability is usually possible. Many cyber liability policies allow for the insured to provide additional insured coverage that are similar to those found in other types of liability policies, such as CGL policies:

> [An entity qualifies as an Additional Insured when]:
>
> 1. any natural person or entity that the Insured Organization has expressly agreed in writing to add as an Additional Insured under this policy prior to the commission of any act for which such person or entity would be provided coverage for under this Policy, but only to the extent the Insured Organization would have been liable and coverage would have been afforded under the terms and conditions of this Policy had such Claim been made against the Insured Organization.[73]

Thus, companies should ensure that contracts with outside vendors potentially posing a cyber security risk include written requirements requiring the company to be added as an additional insured. Additionally, it is a good practice to verify that the vendor's cyber liability policy actually provides for such additional insured coverage.

Moreover, enforceable indemnification agreements from vendors are necessary to provide another layer of protection. Should the additional insured obligation of the vendor fail for lack of coverage or the limits prove inadequate, an enforceable indemnity agreement will provide the company an alternative source of recovery. A contractual indemnification suit can be brought directly against the insured, which may trigger coverage under the cyber liability policy subject to any contractual liability exclusions.

Also, when additional insured coverage is in play, there is often a dispute between which policy should pay first – the additional insured policy or the company's own policy. These disputes often center on both policies' "Other Insurance" clauses. However, an enforceable indemnification agreement will trump the application of Other Insurance clauses, and require that the additional insurer act in primary manner and pay before the businesses' own policy.[74]

- **Practice Tip:** Careful attention should also be given to the language of the indemnification agreement to ensure that it is enforceable. A number Texas courts hold that, in order to be enforceable, the exact harm to be indemnified against must be expressly referenced in the indemnification agreement. These courts have extended the express negligence rule to causes of action beyond negligence, such as warranty claims or strict liability claims.[75] Thus, indemnification for penalties, warranties, and any other claims related to a cyber breach should be included in the language of the indemnification agreement.

III. A Hacker's Anthem – Medical Records Provide The Most Valuable Loot

The danger facing medical companies storing patient health records is like that faced by retailers, but on steroids. The loot for hackers is even more valuable than in the retail sector, as hackers can often obtain social security numbers, dates of birth, and other vital details. Instead of being limited to the number of stolen payment card accounts, hackers with the typical information contained in medical records can open multiple payment accounts, engage in tax and employment fraud, identity theft, and blackmail.

Due to the valuable information contained in these medical records, hackers have honed in on medical companies. This focus has resulted in a rapid increase in data breaches in this sector.[76]

Further fueling the fire is medical companies' widespread adoption of electronic health records in order to reduce medical errors. Unlike its traditional paper-file counterpart, electronic records can be stored in massive quantities, such as millions of files on a single laptop hard drive (which are notoriously easy to lose).

One of the biggest targets in the medical field are health insurers, as they store massive amounts of patient records. These titans stand little chance against a more nimble hacker. Just ask the health insurer, Anthem, Inc., who is the most recent "biggest data breach in history" candidate.[77]

In the Anthem breach, an astonishing **80 million** customer records were compromised.[78] Hackers broke into Anthem's network, and were able to easily make off with this data due to Anthem's failure to encrypt it. As it currently stands, multiple class-action lawsuits have been filed against Anthem relating to the breach. So what are the liabilities that Anthem will likely face?

First, the Health Insurance Portability and Accountability Act ("HIPAA") requires health care providers to maintain security standards for protected

health information. A breach of this statute results in civil penalties and potentially criminal fines.

Additionally, as part of the stimulus bill in 2009, Congress enacted the Health Information Technology for Economic and Clinical Health ("HITECH") Act. This Act strengthens penalties for HIPAA violations. It includes rules for the healthcare industry regarding notifications after a breach, and gave the United States Department of Health and Human Services ("HHS") enforcement powers.[79] Penalties levied by the HHS under the HITECH Act can cost as much as $1.5 million dollars per year.[80]

Moreover, individual states have enacted laws expanding protection mandated by HIPPA and HITECH in several areas. For example, Texas' "Medical Records Act" does not allow a patient's health information to be marketed, or to be used in marketing, without the patient's consent or authorization.[81] Also, the Texas Act imposes its own penalties ranging from $5,000 to $1.5 million per year.[82]

Additionally, patient lawsuits, including class action suits, are a concern. However, patients that have had their medical history exposed have not generally been successful in courts.[83] Patients typically see their cases dismissed under the constitutional doctrine of federal preemption. Healthcare providers argue that because HIPPA did not include a private cause of action, patients attempting to bring state law claims are preempted.

However, the tide may be turning. With some success, patients sidestep this preemption argument by contending that HIPPA is not the basis of their cause of action, but rather probative evidence that the healthcare provide violated the appropriate standard of care under state law.[84] Recently, the Supreme Court of Connecticut rejected the federal preemption argument, and ruled in favor of the patients in an eagerly anticipated decision that has given a shot in the arm to patient claims.[85] It will be interesting to see how the class action lawsuits filed against Anthem fare with regard to the preemption defense.

Thus, the cyber-related claims faced by Anthem will require notification. Companies must ensure that sufficient coverage exists for notifications expenses and fines that a breached company like Anthem will be forced to incur. M, health care companies must be careful in ensuring that the sublimit of their cyber liability policy covering HIPPA/HITECH and state law penalties is sufficient to cover potential penalties that they may be imposed for a catastrophic breach.

Conclusion - If You Build It, They Will Breach It

For companies, a new national Anthem rings loud - it is not a matter of if, but when, companies will fall victim to a debilitating cyber theft. After a breach, companies' ears will be left ringing with the familiar phrase, "Show me the money." Breached businesses may face class action lawsuits from consumers and banks, expensive notification requirements, civil penalties from regulators, and significant business interruption from a crippled or destroyed computer network. Therefore, ensuring that the proper cyber coverage is in place may be the difference between closing the doors, or keeping the lights on.

---

[1] Robert S. Mueller, III, Director, Federal Bureau of Investigation, RSA Cyber Security Conference, San Francisco, CA (Mar. 1, 2012).

[2] Coming soon to companies' CGL policies soon are new cyber exclusion ISO endorsements approved by regulators in most states that leave little room for doubt that most data breach claims are not covered. *ISO Comments on CGL*

Endorsements for Data Breach Liability Exclusions, (Jan. 11, 2014, 2:00 PM), http://www.insurancejournal.com/news/east/2014/07/18/332655.htm. For example, Endorsement CG 21 06 05 14 (Exclusion – Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability – With Bodily Injury Exception) — excludes coverage, under Coverages A and B, for injury or damage arising out of "[a]ny access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information." More importantly, the Endorsement expressly states that no coverage exists for damages "claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by you or others."

[3] One recent case found that no coverage exists for data breaches. *See, e.g., Zurich American Insurance Co. v. Sony Corporation of America*, No. 651982-2011 (N.Y. Sup. Ct. New York Cty.) (filed July 20, 2011) (finding that class action lawsuits stemming from the data breach of Sony's PlayStation Network where personal details from approximately 77 million accounts were stolen did not constitute an alleged "oral or written publication in any manner of material that violates a person's right of privacy" under a CGL policy because Sony did not publish the material the stolen information). The Sony case was on appeal before the intermediate appellate court in New York. Although the case had been fully briefed and argued, the case settled. *Sony, Zurich Reach Settlement in PlayStation Data Breach Case in New York*, (May 11, 2015, 8:00 PM), http:// http://www.insurancejournal.com/news/east/2015/05/01/366600.htm.

Additionally, Travelers filed a declaratory judgment action against P.F. Chang's contesting coverage for three class action lawsuits related to the massive data breach is suffered. *See Travelers Indemnity Company of Connecticut v. P.F. Chang's China Bistro Inc*., case number 2:14-cv-01458, (D. Conn.) (filed Oct. 2, 2014) (contending in its complaint that "[t]he lawsuits fail to trigger coverage under the policies because they do not allege 'bodily injury' or 'property damage' caused by an 'occurrence,' nor do they allege 'advertising injury' or 'personal injury' as the policies expressly and unambiguously define those terms."). Recently, both parties sought to stay the action, as the underlying data breach lawsuits have been dismissed. *Id.* at Doc. 26 (filed Apr. 27, 2015).

[4]Katie Richards, *The 5 Most Embarrassing Revelations From Sony's Sprawling Hack*, (Dec. 13, 2014), http://www.adweek.com/news/advertising-branding/5-most-embarrassing-revelations-sonys-sprawling-hack-161937.

[5] Polly Mosendz, *Malware in Sony Attack 'Undetectable by Industry Standard'*, (Dec. 8, 2014), http://www.newsweek.com/malware-sony-attack-undetectable-industry-standard-290040

[6] *Id.*

[7] (emphasis added.). Katie Benner, *The Sony Hack and the Rise of Cyber Ransoms*, (Sep. 1, 2014), http://www.bloombergview.com/articles/2014-12-24/the-sony-hack-and-the-rise-of-cyber-ransoms. In addition, the hacking group subsequently changed its name from "God'sApstls" to "Guardians of Peace (GOP)." *Id.*

[8] Michael Gregg, *Cyber-Ransom and Online Extortion - 5 Ways You Could Fall Victim*, (Jul. 2, 2014), http://www.huffingtonpost.com/michael-gregg/cyber-ransom-and-online-e_b_5548810.html.

[9] Katie Benner, *Sony Case Among Growing Number of Cyber Ransoms*, (Jan. 1, 2015), http://www.insurancejournal.com/news/national/2015/01/01/351395.htm.

[10] Aarti Shahani, *Ransomware: When Hackers Lock Your Files, To Pay Or Not To Pay?*, (Dec. 8, 2014), http://www.npr.org/blogs/alltechconsidered/2014/12/08/366849122/ransomware-when-hackers-lock-your-files-to-pay-or-not-to-pay.

[11] First Party Computer Security Coverage Endorsement, form E04371, at p. 1 (Dec. 2013 ed.).

[12] Kirsten Acuna, *Sony Has Reportedly Suspended Production On Movies Amid Hack*, (Jan. 11, 2014), http://www.businessinsider.com/sony-shuts-down-filming-on-movies-2014-12.
[13] First Party Computer Security Coverage Endorsement, form E04371, at p. 1 (Dec. 2013 ed.).
[14] Pete Williams, *FBI Says North Korea Was Behind Sony Hack*, (Dec. 19, 2014), http://www.nbcnews.com/storyline/sony-hack/fbi-says-north-korea-was-behind-sony-hack-n271686.
[15] Rory Carroll, *US may put North Korea back on state terror list after Sony 'cybervandalism'*, (Dec. 21, 2014), http://www.theguardian.com/us-news/2014/dec/21/obama-us-north-korea-state-terror-list-sony-hack.
[16] David Lerman, *North Korea Calls Hacking Claim 'Absurd' as U.S. Tightens Sanctions*, (Jan. 2, 2015), http://www.bloomberg.com/politics/articles/2015-01-02/us-slaps-new-sanctions-on-n-korea-in-response-to-sony-hack.
[17] Beazley Breach Response Select, form F00340, at p. 13 (Dec. 2013 ed.), *available at* https://ociaccess.oci.wi.gov/Companyfilings/document?docid=196328&filid=211797.).
[18] (emphasis added). *Sony Pictures CEO says cyber attack cost covered by insurance*, (Jan. 9, 2015), http://www.thestar.com.my/Tech/Tech-News/2015/01/09/Sony-Pictures-CEO-says-cyberattack-cost-covered-by-insuranc/.
[19] Larry Greenemeier, *T.J. Maxx Parent Company Data Theft Is The Worst Ever*, (Mar. 29, 2007), http://www.informationweek.com/tj-maxx-parent-company-data-theft-is-the-worst-ever/d/d-id/1053522?.
[20] Tom Espiner, *Wi-Fi hack caused TK Maxx security breach*, (May 8, 2007), http://www.zdnet.com/article/wi-fi-hack-caused-tk-maxx-security-breach/.
[21] Kelli B. Grant, *Why did Target take so long to report the breach?*, (Dec. 20, 2013), http://www.cnbc.com/id/101287567#.
[22] Brian Krebs, *Target Hackers Broke in Via HVAC Company*, (Feb. 5, 2014, 2:00 PM), http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.
[23] Rachel Abrams, *Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop*, (Aug. 5, 2014), http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html?_r=0.
[24] Shelly Banjo, *Home Depot Hackers Exposed 53 Million Email Addresses*, (Nov. 6, 2014), http://www.wsj.com/articles/home-depot-hackers-used-password-stolen-from-vendor-1415309282.
[25] *Id*.
[26] Jeremy Kirk, *Home Depot spent $43 million on data breach in just one quarter*, (Nov. 25, 2014), http://www.pcworld.com/article/2852472/home-depot-spent-43-million-on-data-breach-in-just-one-quarter.html.
[27] Robert McMillan, *Restaurants sue vendors after point-of-sale hack*, (Dec. 1, 2009), http://www.computerworld.com/article/2521259/security0/restaurants-sue-vendors-after-point-of-sale-hack.html.
[28] As of January 1, 2015, the only states without similar breach notification laws are Alabama, New Mexico and South Dakota. However, a one-size-fits all approach may be coming soon. The Obama administration proposed federal legislation that would supersede these varying state regulations. Rachael King, *30 Days Not Enough Time in Obama's Proposed Breach Notification Law: Retail Group*, (Jan. 12, 2015, 8:00 PM), http://blogs.wsj.com/cio/2015/01/12/30-days-not-enough-time-in-obamas-proposed-breach-notification-law-retail-group/.
[29] For example, the Texas statute defines personal identifiable information as "an individual's first name or first initial and last name in combination with any one or more of the following items, if the name in the items are not encrypted: … Social Security number, driver's license number or other government issued identification number, account or card numbers in combination with the required access or security codes. TEX. BUS. & COM. CODE § 521.002 (Vernon).

[30] *Id.* at § 521.052-053
[31] Tim Stapelton, *Data Breach Cost*, (Jul. 2012), http://www.zurichna.com/internet/zna/sitecollectiondocuments/en/products/securityandprivacy/data%20breach%20costs%20wp%20part%201%20%28risks,%20costs%20and%20mitigation%20strategies%29.pdf.
[32] Privacy liability insurance is often paired in the same insuring agreement with "network security liability" coverage. Network security coverage is designed to protect policyholders when there is an unauthorized access to the insured's computer network.
[33] Furthermore, the fact that a company's discovery of a data breach must be reported dovetails with the "claims-made" nature of typical cyber liability policies. For coverage to be triggered, an insured company must discover and report the data breach during the applicable policy period. Failure to tender the data breach to the insurer within the policy period is likely fatal to coverage under the policy. *See Prodigy Communications Corp. v. Agric. Excess & Surplus Ins. Co.*, 288 S.W.3d 374, 378-79 (Tex. 2009).
[34] TEX. BUS. & COM. CODE ANN. § 521.151(a-1) (Vernon).
[35] *See*, e.g., Beazley Breach Response Select, form F00340, at p. 2, §3 (Dec. 2013 ed.).
[36] TEX. BUS. & COM. CODE ANN. § 521.151 (Vernon).
[37] *See* Section 5 of the FTC Act, 15 U.S.C. § 45.
[38] Given the limited authority the FTC relies upon, a number of companies have challenged the FTC's authority, including Wyndham hotels. To date, these arguments have not been successful. In particular, on April 7, 2013, the U.S. District Court for the District of New Jersey ruled in favor of the FTC, holding that it had authority under the "unfairness" prong of the FTC Act to bring an enforcement action against Wyndham for its alleged unreasonable data security practices. *F.T.C. v. Wyndham Worldwide Corp.*, 2014 WL 1349019 (D.N.J. Apr. 7, 2014), *motion to certify appeal granted* (June 23, 2014). Recently, the Third Circuit affirmed the district court's holding, and found that the FTC had authority to bring enforcement actions relating to data breaches. *F.T.C. v. Wyndham Worldwide Corp*., 2015 WL 4998121 (3d Cir. Aug. 24, 2015).
[39] Beazley Breach Response Select, form F00340, at p. 7 (Dec. 2013 ed.).
[40] *Compare Bullock v. Md. Casualty Co.*, 85 Cal.App.4th 1435, 1448 (2001) (reasoning that civil penalties for violation of city ordinance did not trigger duty to defend because "public policy would not permit defendants to insure those sums"); *with Wilson v. Chem–Solv, Inc.*, 1988 WL 109375, *1 (Del.Super.Ct. 1988) (concluding that public policy did not bar insurance coverage for civil penalties assessed for pollution).
[41] *Fairfield Ins. Co. v. Stephens Martin Paving, LP*, 246 S.W.3d 653 (Tex. 2008).
[42] *Id.* at 670.
[43] *Id.*
[44] 47 U.S.C. § 227.
[45] *Columbia Cas. Co. v. HIAR Holding, L.L.C.*, 411 S.W.3d 258, 274 (Mo. 2013) (finding that the penalties were insurable because the insured's "conduct … was not willful and malicious, but rather it was negligent and unintentionally resulted in violations of the TCPA."); *Standard Mut. Ins. Co. v. Lay*, 2013 IL 114617, ¶ 35, 989 N.E.2d 591, 600 (Ill. 2013) (same); *Motorists Mut. Ins. Co. v. Dandy-Jim, Inc.*, 912 N.E.2d 659 (Ct. App. Oh. 2009) (same); *but see Terra Nova Ins. Co. v. Fray-Witzer*, 869 N.E.2d 565 (Mass. 2007)(holding that TCPA $500 damages are insurable, but if penalties above $500 were awarded pursuant to the treble damages provision, "such an increase would amount to punitive damages and would not be covered.").
[46] In 2006, five major credit card brands (Visa, MasterCard, American Express, Discover Financial Services and JCB International) created the Payment Card Industry Security Standards Council to address issues of payment security.

[47] Software vendors of POS systems are governed by a similar standard developed by the major payment card brands, PCA-DSS.
[48] *PCI Faqs*, https://www.pcicomplianceguide.org/pci-faqs-2/.
[49] *See* Beazley Breach Response Select, form F00340, at p. 1 (Dec. 2013 ed.).
[50] Beyond notification laws, only a few states have laws that impose fines on companies that are not PCI-DSS compliant. In these states, such as Nevada, regulatory fines can be levied against companies that are not PCI-DSS compliant. *See* NEV. REV. STAT. § 603A.215. However, at the present, Texas does not have a similar statute mandating PCI-DSS compliance. Should a company find itself in the crosshairs of these statutes, coverage under a cyber liability policy would likely exist under "PCI Fines and Costs" coverage provision.
[51] The Black Card was popularized by the movie starring George Clooney, "Up in the Air."
[52] *US banks have re-issued 17.2 million cards following Target data breach*, (Feb. 7, 2014), http://www.finextra.com/news/fullstory.aspx?newsitemid=25702.
[53] Jonathon Randles, *Target Data Breach Ruling Raises Stakes For Retailers*, (Dec. 4, 2014), http://www.law360.com/articles/600931/target-data-breach-ruling-raises-stakes-for-retailers.
[54] Prior to the consolidation into the MDL, Target faced over 100 lawsuits in federal district courts across the nation related to the data breach.
[55] *See In re Target Corp. Customer Data Security Breach Lit.*, 2014 WL 6775314 (D. Minn. Dec. 2, 2014).
[56] *Id.*
[57] Ahiza Garcia, *Target settles for $39 million over data breach*, (Dec. 2, 2015), http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/
[58] *Id.*
[59] *In re Target Corp. Customer Data Sec. Breach Litig.*, MDL 14-2522 PAM/JJK, 2015 WL 5432115, at *7 (D. Minn. Sept. 15, 2015).
[60] B. Dan Berger, *Congress Must Make Retailers Responsible for Data Breaches*, (Jan. 15, 2014), http://www.americanbanker.com/bankthink/congress-must-make-retailers-responsible-for-data-breaches-1064921-1.html.
[61] For example, Minnesota's Plastic Card Security Act provides:

> No person or entity conducting business in Minnesota that accepts a[] [credit or debit card] in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.
> * * * *
> Whenever there is a breach of the security of the system of a person or entity that has violated this section . . . that person or entity shall reimburse the financial institution that issued any [credit or debit cards] affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders . . . .

MINN. STAT. § 325E.64, subd. 2, 3.

[62] Specifically, the proposed Texas bill, H.B. No. 3222, provided:

> A business that, in the regular course of business, collects, maintains, or stores sensitive personal information in connection with an access device must comply with payment card industry ["PCI"] data security standards ["DSS"].
> …[and]…
> A financial institution may bring an action against a business that is subject to a breach of system security if, at the time of the breach, the business is [not in compliance with PCI DSS].

[63] Beazley Breach Response Select, form F00340, at p. 1 (Dec. 2013 ed.).
[64] *See Katz v. Pershing, LLC*, 672 F.3d 64 (1st Cir. 2012); *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011).
[65] *See Krottner v. Starbucks Corp*., 628 F.3d 1139 (9th Cir. 2010); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629 (7th Cir. 2007).
[66] 133 S. Ct. 1138 (2013).
[67] *Id*. at 1151.
[68] *Storm v. Paytime, Inc.*, 2015 WL 1119724, at *6 (M.D. Pa. 2015) (finding no standing under *Clapper*, and holding that "[p]laintiffs do not allege that they have actually suffered any form of identity theft as a result of the data breach—to wit, they have not alleged that their bank accounts have been accessed, that credit cards have been opened in their names, or that unknown third parties have used their Social Security numbers to impersonate them and gain access to their accounts. In sum, their credit information and bank accounts look the same today as they did prior to Paytime's data breach in April 2014."); *Lewert v. P.F. Chang's China Bistro, Inc.*, 2014 WL 7005097, at *3 (N.D. Ill. Dec. 10, 2014) (dismissing lawsuit for lack of standing under *Clapper* and holding that "[s]peculation of future harm does not constitute actual injury."); *In re Science Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig*., 2014 WL 1858458 (D.D.C. May 9, 2014) (same); *Strautins v. Trustwave Holdings, Inc*., 2014 WL 960816 (N.D. Ill. Mar. 12, 2014) (same); *Galaria v. Nationwide Mut. Ins. Co*., 2014 WL 689703 (S.D. Ohio Feb. 10, 2014) (same); *Polanco v. Omnicell, Inc*., 2013 WL 6823265 (D.N.J. Dec. 26, 2013) (same); *In re Barnes & Noble Pin Pad Litig*., 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013) (same); *but see In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 2014 WL 223677 (S.D. Cal. Jan. 21, 2014) (finding standing in the face of *Clapper*); *In re Adobe Sys., Inc. Privacy Litig.*, 2014 WL 4379916 (N.D. Cal. Sept. 4, 2014) (same); *Moyer v. Michaels Stores, Inc.*, 2014 WL 3511500, at *5 (N.D. Ill. July 14, 2014).
[69] *See In re Target Corp. Customer Data Security Breach Lit*., MDL No. 14-2522-PAM, Doc #281 (D. Minn., Dec. 18, 2014).
[70] *Id.*
[71] *Target agrees to pay $10 million to settle lawsuit from data breach*, (Mar. 19, 2015), http://www.reuters.com/article/2015/03/19/us-target-settlement-idUSKBN0MF04K20150319; *and See Order Preliminarily Approving Settlement, In re Target Corp. Customer Data Security Breach Lit*., MDL No. 14-2522-PAM, Doc #364 (D. Minn., Mar. 19, 2015).
[72] *Id.*
[73] Beazley Amendatory Endorsement, form E04418 (Dec. 2013 ed.).
[74] *See American Indem. Lloyds v. Chartis Prop. & Cas. Ins. Co.*, 335 F.3d 429, 436 (5th Cir. 2003) ("[T]he clear majority of jurisdictions recognizes the foregoing exception and gives controlling effect to the indemnity obligation of one insured to the other insured over 'other insurance' or similar clauses in the policies of the insurers, particularly where one of the policies covers the indemnity obligation."); *Northfield Ins. Co. v. Lexington Ins. Co*., 2003 WL 22138440 at *7 (S.D. Tex. 2003) ("The court concludes that Lexington's [CGL *and* Umbrella] policies are

the primary policies and that Lexington may not seek contribution from Northfield."); *Wal-Mart Stores, Inc. v. RLI Ins. Co.*, 292 F.3d 583, 593-94 (8th Cir. 2002) (same).

[75] *See Houston Lighting & Power Co. v. Atchison, Topeka & Santa Fe Ry. Co.*, 890 S.W.2d 455, 458–59 (Tex.1994) (extending express negligence test to strict liability claims); *and Staton Holdings, Inc. v. Tatum, L.L.C.*, 345 S.W.3d 729, 734 (Tex. App.—Dallas 2011, pet. denied) (same regarding warranty claims).

[76] For example, there was a shocking 138% increase in data breaches between from 2012 to 2013. Redspin, *Redspin Breach Report 2013: Protected Health Information*, (Feb. 2014), https://www.redspin.com/resources/whitepapers-datasheets/Request-2013-Breach-Report-Protected-Health-Information-PHI-Redspin.php.

[77] Under the Anthem umbrella of companies are Amerigroup, Anthem and Empire Blue Cross Blue Shield companies, Caremore, and Unicare.

[78] *Anthem breach highlights need for dynamic access control, says KuppingerCole*, (Apr. 21, 2015), http://www.computerweekly.com/news/4500244712/Anthem-breach-highlights-need-for-dynamic-access-control-says-KuppingerCole.

[79] A violation of HIPPA is presumed to be a breach unless the covered entity demonstrates that there is a low probability that the protected healthcare information has been compromised. *See* 11 HITECH Act § 13402, codified at 42 U.S.C. 17932(g).

[80] In addition, HITECH extends HIPAA violation liability to health-care vendors to whom protected health information is disclosed. This expansion of entities that must comply with HIPPA and HITECH includes third-party administrators or accounting firms. Thus, the world of companies that must comply with HIPPA has expanded exponentially.

[81] *See* TEX. HEALTH & SAFETY CODE ANN. § 181.152 (Vernon).

[82] *Id.* at § 181.201 (Vernon).

[83] *See, e.g., Bonney v. Stephens Memorial Hospital*, 2011 ME 46, p.20 (Me. 2011) (holding that because HIPAA does not provide a private cause of action, it cannot create a standard for violation of state common law); *Young v. Carran*, 289 S.W.3d 586, 588 (Ky. Ct. App. 2008) ("HIPAA does not create a state-based private cause of action for violations of its provisions").

[84] *See, e.g., R. K. v. St. Mary's Med. Ctr., Inc.*, 229 W. Va. 712, 718–21 (W. Va. 2012) (using HIPAA as standard of care for breach of medical confidentiality); *Acosta v. Byrum*, 180 N.C. App. 562, 568 (N.C. Ct. App. 2006) (same); *I.S. v. Washington Univ.*, 2011 U.S. Dist. LEXIS 66043, at *16 (E.D. Mo. June 14, 2011) (same); *K.V. v. Women's Healthcare Network, LLC*, 2007 U.S. Dist. LEXIS 102654, at *2 (W.D. Mo. June 6, 2007) (same with regards to a negligence per se claim); *Harmon v. Maury County, TN*, 2005 U.S. Dist. LEXIS 48094, at *11 (M.D. Tenn. Aug. 31, 2005) (same)*; Doe v. Southwest Cmty. Health Ctr.*, 2010 Conn. Super. LEXIS 2167, at *25–26 (2010) (same); *Fanean v. Rite Aid Corp. of Delaware, Inc.*, 984 A.2d 812, 817 (Del. Super. Ct. 2009) (same); *and see Baum v. Keystone Health Plan*, 826 F.Supp.2d 718, 721 (E.D. Pa. 2011); *Yath v. Fairview Clinics, N.P.*, 767 N.W.2d 34, 49–50 (Minn. Ct. App. 2009) (holding Minnesota statute not preempted by HIPAA).

[85] *Byrne v. Avery Center for Obstetrics & Gynecology, P.C.*, 2014 Conn. LEXIS 386 (Conn. Nov. 1, 2014).