CLM Claims & Litigation Management Alliance™
ADVANCING ETHICS, COOPERATION AND EDUCATION

CLM 2015 Cyber Liability Summit
October 21, 2015 in New York City

The Retail Data Breach – Navigating the Murky Waters of the Payment Card Industry

I. PCI-DSS Overview

PCI-DSS Objectives

The goal of PCI DSS is to protect cardholder data whenever it is processed, stored or transmitted. Sensitive authentication data (magnetic stripe data, chip data, CAV2/CID/CVC2/CVV2) must never be stored after authorization.

Payment Card Industry Data Security Standards (PCI DSS) are administered by the PCI Security Standards Council, which was founded by VISA, MC, AMEX, DISCOVER, and JCB.

PCI DSS applies to all entities that store, process or transmit credit card data.

PCI / Merchant Relationships

The Players

- Issuing Bank
  Bank that issues payment cards to consumers (cardholders)

- Acquiring Bank
  Contracts for payment services with merchant; merchant must validate PCI DSS compliance with its "acquirer"; acquirer reports compliance status to card associations

- Merchant
  Entity that sells goods/services and accepts cards; responsible for safeguarding credit card data and complying with the PCI DSS

- Service Provider
  Entity that provides all or some of the payment services for the merchant; responsible for safeguarding credit card data and complying with the PCI DSS

- PCI Security Standards Council (PCI SSC)

Founded by card associations and responsible for administering PCI DSS

- PCI Data Security Standards (PCI DSS)
  Technical and operational requirements set by PCI SSC to protect cardholder data

- Cardholder
  Person holding a credit or debit card

- Card Associations (Brands) – VISA,MC, AMEX, Discover, JCB
  Enforce compliance with the PCI DSS

II. Data Security Standards in PCI

Standard that is applied to Merchants, Service Providers (Third Third-party vendor, gateways) and Systems (Hardware, software) that stores cardholder data, transmits cardholder data, processes cardholder data and applies to electronic transactions as well as paper transactions.

PCI 3.0

- Inventory of system components in scope for PCI DSS to support development of configuration standards.
- Evaluate evolving malware threats for any systems not considered to be commonly affected by malicious software.
- Coding practices to protect against broken authentication and session management (effective 7/1/15).
- Service providers must use unique authentication credentials when for each of their customers (effective 7/1/15).
- Control physical access to sensitive areas for onsite personnel, including a process to authorize access, and revoke access immediately upon termination.
- Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution (effective 7/1/15).
- Implement methodology for penetration testing.

PCI DSS Principles

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

3. Protect stored data.
4. Encrypt transmission of cardholder data and sensitive information across public networks.

Maintain a Vulnerability Management Program

5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data.
11. Routinely test security systems and processes.

Maintain an Information Security Policy.

12. Establish high-level security principles and procedures.

Visa and MasterCard Validation Requirements

Level 1-Visa/MasterCard-- Annual onsite review by merchant's internal auditor or a Qualified Security Assessor (QSA) or Internal Audit if signed by Officer of the company, and a quarterly network security scan with an Approved Scanning Vendor (ASV).

Level 2-- Completion of PCI DSS Self Assessment Questionnaire annually, and quarterly network security scan with an approved ASV.

Level 3-- Completion of PCI DSS Self Assessment Questionnaire annually, and quarterly network security scan with an approved ASV.

Level 4-- Completion of PCI DSS Self Assessment Questionnaire annually, and quarterly network security scan with an approved ASV.

Submit summary of PCI compliance plan, via acquirer, by July 30, 2007. If a breach has been reported, or found, Visa reserves the right to move the Level 4 merchant to a Level 1. If so, the Level 4 merchant must abide by the Level 1 validation requirements.

III. Responding to a PCI Occurrence

Investigation

The primary focus of an investigation is to confirm the indicated avenue of the event and identify the post event network activity related to system infiltration and data exfiltration. Additionally, the compromise investigation identifies additional compromised endpoints and user accounts.

- Understand potential breadth and scale of the incident
- Identify locations of potentially compromised systems
- Identify and examine logs available for the incident
- Determine any priority systems or logs with a tier based system for further collection and examination

- Identify if an immediate, remote assessment or collection is required.

Damage Assessment

The damage assessment focuses on ascertaining the data accessed or exposed, as well as providing an understanding of what the adversary sought, and what relevant issues will need to be addressed in future actions. The damage assessment can also provide further guidance on the impact of the data exfiltration on the victim's operations.

- Files accessed
- Indicators of file use and adversary intelligence gathering
- Files potentially or actually exfiltrated
- Adversary's next steps

The PCI Forensic Investigation

The PCI Forensic Investigator (PFI) program establishes and maintains rules and requirements regarding eligibility, selection and performance of companies that provide forensic investigation services to ensure they meet PCI Security Standards. The PFI program aims to help simplify and expedite procedures for approving and engaging forensic investigators by:

- Providing a single set of requirements for forensic investigators upon which market participants may align
- Maintaining a list of Council-approved forensic investigators for compromised entities to choose from
- Providing guidance on how investigations are to be conducted and reported

While your client or insured pays for the PFI, the PFI reports to the PCI and is not looking out for your client or insured's best interests.

IV. Legal Issues

Attorney as Quarterback

A significant concern of organizations is that the written reports generated at the culmination of security risk assessments, whether conducted internally or by an external party, may provide a roadmap for an adversary in some future proceeding. It is important for organizations seeking to protect such reports from unwanted discovery.

Organizations can attempt to cloak a risk assessment from disclosure by employing legal counsel to manage the review process. In this scenario, counsel would be retained by the organization to provide legal advice regarding data security exposures, and to develop a strategy for risk minimization. As part of this process, counsel, rather than the organization, would retain an independent cyber consultant to assist in the due diligence analysis and in the preparation of a cyber risk assessment report detailing the organization's vulnerabilities, threats and lack of controls, as well as recommendations for addressing these issues. The report would be

addressed to counsel, which would then be incorporated into a more comprehensive report for the organization.

First Party Issues

First-party damages are typically defined as damages suffered by policyholders to their own property. If a first party policy holder / property owner suffers damage to its own computer systems, network, and (in some cases) software applications, a claim will be filed under the first party insurance policy. These first party claims are typically for the replacement cost or remediation estimated cost associated with the damaged property.

State Notice Laws

On April 10, 2014, Kentucky became the 47th state to enact data breach notification laws. The new Kentucky law applies to "Information Holder[s]," defined as a persons or business entities that conduct business in Kentucky, including both those that own the personal information they maintain and those that maintain personal information for third parties.

The new law requires notification of the affected class of a data beach "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement". While the new law does not require notice to the Kentucky Attorney General or other any other state regulator, it does require notification to the consumer reporting agencies, again, "without unreasonable delay" if more than 1,000 Kentucky residents are impacted.

New Mexico is one of the three remaining states without data breach notification laws in place. However, H.B. 224, the newly proposed legislation would require businesses to notify customers of any breach allowing access to unencrypted personal information within 45 days. The law also requires notification to the state attorney general if more than fifty residents of the state are affected. Should New Mexico's bill be made law, Alabama and South Dakota would be the only states left without data protection laws in place.

Multiple states have also proposed legislation to strengthen laws already in place.

Florida law provides that companies must provide notification to its customers if it has reason to believe that its customers' private information ("PI") was accessed by someone not authorized to access such information. In particular, Fla. Stat Ann. Ch. 817.568, § 501.171 (2014) provides that notification "must be given to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been improperly acquired by an unauthorized person". Additionally, notice must be provided to the Department of Legal Affairs if the breach affects 500 or more individuals. The law further requires reporting to appropriate consumer protection agencies when a breach results in notification to an affected class of 1,000 or more people.

Third Party Issues

Litigation & Article III Standing

The Seventh Circuit Court of Appeals' recent ruling in *Remijas v. Nieman Marcus*, 2015 U.S. App. LEXIS 12487 (7th Cir. July 20, 2015), reversed the lower court and held that customers of luxury retailer Neiman Marcus had alleged sufficient injury to demonstrate their constitutional standing despite the fact that only a portion of the putative class had actually been subject to fraudulent charges.

The 2013 U.S. Supreme Court decision in *Clapper v. Amnesty International USA,* 133 S. Ct. 1138 (2013), interpreting Article III standing requirements for damages to be "certainly impending" is routinely the basis of data breach class action defendants' efforts to challenge the plaintiffs' constitutional standing arguing that while the plaintiffs' personal data may have been compromised, there are no actual damages since individual plaintiffs do not typically pay for credit monitoring, fraudulent charges or credit card replacement costs.

Multiple class-action complaints were filed against Neiman Marcus following its 2013 data breach. The matters were consolidated in June 2014 under four named plaintiffs alleging four different categories of actual injury: (1) lost time and money resolving fraudulent charges; (2) lost time and money protecting against future identity theft; (3) the financial loss of buying items at Neiman Marcus that they would not have purchased had they known of the store's careless approach to cybersecurity; and (4) lost control over the value of their personal information. The plaintiffs also alleged a likelihood of imminent future injury based on an increased risk of future fraudulent charges and a greater susceptibility to identity theft.

In September 2014, the U.S. District Court for the Northern District of Illinois in Chicago dismissed the case for lack of Article III standing based primarily on the principles set forth by Clapper.

In its reversal, the appellate court first found that the 9,200 putative class members who actually incurred fraudulent charges had demonstrated a concrete injury, despite already being reimbursed for those charges, because they had "suffered the aggravation and loss of value of the time needed to set things straight, to reset payment associations after credit card numbers are changed, and to pursue relief for unauthorized charges." This is not really a departure from prior data breach cases as courts have long held that remediation expenses arising from an actual, concrete injury are, themselves, considered a concrete injury.

With respect to the approximately 340,000 other putative class members the Court expressed disagreement with the recent approach applied in other jurisdictions to summarily dismiss claims of future injury pursuant to Clapper. The Seventh Circuit noted that "Clapper does not, as the district court thought, foreclose any use whatsoever of future injuries to support Article III standing" and recognized that Clapper "did not jettison the 'substantial risk' standard" which allows for standing based on a substantial risk that the harm will occur, thereby prompting the "plaintiffs to reasonably incur costs to mitigate or avoid that harm."

Referencing other cases as persuasive examples of the principle applied in a mass data breach context, the Seventh Circuit reasoned that "there is no need to speculate as to whether the Neiman Marcus customers' information has been stolen," and that Neiman Marcus customers should not have "to wait for the threatened harm to materialize in order to sue."

Interestingly, the Court appeared to distinguish data breach litigation generally, as opposed to the governmental monitoring in Clapper, to conclude that past and future damages can sometimes be inferred from the nature of security hacks and the circumstances surrounding a particular breach. For example, the Court found it "plausible to infer" that hackers break into customer databases for the purpose of making fraudulent charges or stealing identities, and that such injuries can occur up to a year or more after the initial breach.

Further, the court found it "telling" that Neiman Marcus did not contest that the breach occurred and had offered to provide a full year of credit-monitoring services to all of the potentially affected customers. This, the court concluded, could be construed as a sign that the risk of future fraudulent charges or identity theft for the entire class was more than merely speculative.

The Court also found that the over 340,000 class members who had not already been defrauded had further established standing to sue based on the "time and money" spent "protecting themselves against future identity theft and fraudulent charges." Although Clapper held that plaintiffs "cannot manufacture standing by incurring costs in anticipation of non-imminent harm," the Seventh Circuit again distinguished the card-replacement and credit monitoring costs associated with data breach cases as more of a "concrete injury" rather than a questionable precaution.

As for causation, the Court dismissed Neiman Marcus' argument that the plaintiffs' injuries might have been caused by one or more of the several other large data breaches that occurred around the same time as the one at Neiman Marcus. Citing recent decisions, the court noted that it is "certainly plausible for pleading purposes" that the injuries be "fairly traceable" to the Neiman Marcus breach. The Court again referred to Neiman Marcus' recognition of the breach and exposure of credit and debit card information, notice to the class of the potential risk, and offer of credit monitoring services. "Those admissions and actions," said the Court, "adequately raise the plaintiffs' right to relief above the speculative level."

Finally, the Court concluded that partial reimbursement for the discovered fraudulent charges does not necessarily mean that the class cannot seek reimbursement for its mitigation expenses or future injuries, and fails to account for the varying degrees of damages suffered by credit cardholders as opposed to debit cardholders.

The Remijas decision is particularly noteworthy due to its apparent departure from recent data breach class action rulings.

It will be interesting to see how this case is adopted and/or distinguished in other judicial circuits, and whether it will force a circuit split to be resolved by the U.S. Supreme Court. Notably, *Spokeo, Inc. v. Robins*, No. 13-1339, cert. granted 135 S. Ct. 1892 (2015), is expected to be decided by the Supreme Court next fall. Although the issue in Spokeo is technically limited to whether Congress may confer Article III standing upon a plaintiff based on the defendant's "bare violation of a federal statute," the Supreme Court may use the opportunity to clarify some of the "speculative" and "hypothetical" injury issues discussed in Clapper.

Assessments / Fines / Penalties

These penalties are not levied by PCI Security Council itself, but rather, the fines levied are by Card Associations themselves against the merchant bank, which then passes fines on to merchant.

Fines for security breach

Visa - Up to $500,000 per occurrence
MC – Up to $500,000 per occurrence

Amount of fines dependent upon

Number of card numbers stolen
Circumstances surrounding incident
Whether Track Data was stored or not
Timeliness of reporting incident

V. Takeaways (5 Minutes)

A. Advances in Technology
    a. Software as a Service
    b. Internet of Things
B. Sophisticated Marketplace
    a. Broker sophistication
    b. Cyber in the Headlines
    c. Educated marketplace
C. Mobility
D. Big Data