Credit Card Data Breaches: Protecting Your Company from the Hidden Surprises

By

David Zetoony
Partner, Bryan Cave LLP

Courtney Stout
Counsel, Davis Wright Tremaine LLP

With Contributions By

Suzanne Gladle, ARM
Director, Cyber Program Operations
McGriff, Seibels & Williams, Inc.

Table of Contents

Part I: Assessing the Risk to a Retailer from a Credit Card Data Breach

Debit and credit cards are now the primary form of retail payment. One source estimates that 60% of all retail transactions involve a payment card – far usurping cash or checks as the preferred method of payment.[1] Most retailers do not realize, however, that by accepting credit cards they expose themselves to the risk of a data security breach and significant potential costs and legal liabilities. This whitepaper explains the key risks that a retailer faces following a data security breach of their payment card systems as well as the potential for addressing some of those risks through the purchase of cyber-insurance.

1. What are a retailer's major sources of direct costs (first party costs or claims) following a data breach?

Retailers typically incur significant direct costs upon experiencing a payment card data breach. These often include the following investigation and external vendor costs.

PCI Certified Forensic Investigator. The payment brand's operating rules permit them to require that a retailer retain one of 14 forensic investigators that is certified by the payment card industry ("PCI") council. These PCI-certified forensic investigators ("PFIs") must be paid for by a retailer, but are required to report their findings to the payment brands. Those findings include the opinion of the PFI as to whether the retailer was in compliance with the PCI data security standards at the time that the breach occurred, when the breach began, how long the breach lasted, and the number of payment cards that may have been exposed in connection with the breach. The payment brands use these findings as a basis for imposing these fees.

Myth: Retailers have little exposure from a breach of credit card data because card processors bear the primary responsibility for a breach.

Fact. In addition to the normal repercussions of a data security breach (reputation damage, the risk of class action litigation, the risk of a regulatory investigation, and the cost of investigating the breach), if a retailer's credit card system is compromised, the retailer may be contractually liable to its payment processor, its merchant bank, and ultimately the payment card brands (VISA, MasterCard, and American Express).

Privileged Forensic Investigator. In addition to a PFI, many retailers choose to retain a second forensic investigator. The second investigator is often retained by the retailer's law firm or general counsel and is used to help provide the retailer's attorneys with facts and information necessary for them to provide legal advice to the retailer. For example, the privileged forensic investigator may review the reports and conclusions of the PFI and provide their opinion as to whether the PFI's analysis is accurate.

Outside Counsel. Outside counsel is typically needed to negotiate agreements between the retailer, the PFI, and the Privileged Forensic Investigator. Outside counsel also

[1] Claes Bell, "Cash No Longer King In Retail," Bankrate.com (June 6, 2012).

provides advice and counseling concerning the potential for the third party claims discussed in the next section, and how to minimize any liability relating to such claims.

Public Relations/Crisis Management. Many retailers retain public relations firms that specialize in crisis communications or specifically in communicating data security breaches to help them disclose the data breach in a manner that minimizes the impact the incident has to the retailer's brand.

Consumer Notification. Many retailers decide to communicate information about a payment card breach to impacted consumers. There are a variety of ways in which such communications can be made. If the retailer decides to communicate directly with consumers, depending upon the quantity of consumers, they may incur significant printing and mailing costs. In addition, some retailers choose to offer impacted consumers credit monitoring, identity theft protection services, or identity theft insurance. The type of services offered, and the duration for which they are offered, impact cost.

2. What are a retailer's major sources of liability (third party claims) following a data breach?

Following a payment card data breach, retailers often face three forms of liability from third parties: payment card brand fees, regulatory exposure, and class action exposure. Each of these third party liabilities is summarized below.

Payment Card Brand Fees. Many retailers mistakenly believe that they have no payment card industry ("PCI") related data on their systems, and that their payment processor will be liable for any damage arising from a payment card related data breach. Even if the retailer does not knowingly store PCI data, the fact that it is collected by the retailer at the point of sale means that the data exists on the retailer's network – even if for an extremely short amount of time, sometimes no longer than a millisecond. That is often long enough for malware deployed by hackers to capture payment card data. Indeed, in the past five years the vast majority of credit card breaches reported by retailers involve a type of malware referred to as "ram-scraping," which operates by capturing a consumer's credit card information right after a credit card is swiped and before it is transferred to the retailer's payment processor.

When payment card information is stolen from a retailer it can trigger a series of contractual liabilities that exists across the payment card ecosystem. Specifically, payment brands (Visa, MasterCard, and Discover) have created a number of penalties that they impose upon the banks with which they do business following a credit card breach at a retailer. These penalties take many different forms and are described under many different names by the payment brands. Although they are collectively referred to in this paper as "fees," the following provides an example of the different categories of penalties that can be imposed by just one payment brand:

The payment brands can assess more than 25 different contractual penalties, fines, adjustments, fees, and charges upon a retailer following a PCI data security breach.

- Security Requirements Noncompliance Fee. Discover Merchant Operating Regulations (Release 14.1) Rules 14.3.2, 14.3.3, 14.4, 17.6
- Validation of Security Requirements Noncompliance Fee. Discover Merchant Operating Regulations Rules (Release 14.1) Rule 14.2
- Data Security Breach Fee. Discover Merchant Operating Regulations (Release 14.1) Rule 14.3.3
- Other Fees and Penalties. Discover Merchant Operating Regulations (Release 14.1) Rule 17.6

Although they are referred to under many different names, most of the fees are purportedly designed to reimburse the payment brands for costs that they may incur as a result of a breach that occurs at a retailer. The payment brands impose the fees on the merchant bank that permitted the retailer to access the payment card networks, and with whom the payment brands have a contractual relationship.

Although the fees are imposed on merchant banks, merchant banks are not expected to pay them. Almost all merchant banks protect themselves from the cost of the fees by contractually requiring the third party payment processors that work directly with a retailer to process credit card transactions to reimburse the bank if fees are assessed. Third party payment processors, in turn, protect themselves by contractually requiring that a retailer reimburse them for the fees. As a result, most retailers end up paying the full cost of the fees imposed by the payment brands.

Myth: Every data breach results in a class action.

Fact: Most data breaches do not result in litigation. In fact, only 4% of publicly reported data breaches lead to class action lawsuits. Furthermore, the largest and most publicized breaches often act as "lightning rods" which draw multiple complaints by different plaintiff's attorneys.

Source: Bryan Cave LLP's *2015 Data Breach Litigation Report: A Comprehensive Analysis of Class Action Lawsuits Involving Data Security Breaches Filed in United States District Courts*.

Regulatory Costs. Numerous federal and state agencies have overlapping jurisdiction over retailers. This includes, among others, the FTC, the SEC, and State Attorneys General. When a large-scale payment card breach occurs, it is not unusual for more than one agency to investigate the incident.

Class Action Litigation. The retail industry is disproportionately targeted by the plaintiff's bar following a payment card data breach. Specifically, while only 14.5% of publicly reported breaches relate to the retail industry, nearly 80% of data security breach class actions target retailers. While plaintiff's attorneys have alleged 24 different legal theories, there is a growing bias toward lawsuits primarily premised upon negligence, contract, deception, or unfairness legal theories.

Although the majority of suits that are filed following a payment card breach are dismissed or settled, the costs to defend and settle such claims can be significant.[2]

Myth: If a vendor causes a credit card breach, the vendor will bear all responsibility for damages.

Fact: Under the payment card brand regulations and many card processing agreements, the retailer is fully responsible for any "downstream" third party vendor breach of PCI data (card number or sensitive authentication data). Your negotiated contract terms with each third party vendor that touches your PCI data will govern what you can recover from your vendor if they are the source of a data breach of your customers' credit card data.

3. Is a retailer shielded from liability by its card processor or device manufacturers?

Many retailers believe that they will not have liability for a payment card data breach because the companies that provided them with the services, hardware, or software that they use to process credit card transactions will be responsible in the event of a data security breach. Just like with any contract, the "fine print" in the contracts for these products or services typically include a number of provisions that place the liability for a breach on the retailer. These include:

- The processor's or device manufacturer's liability for any data breach is often limited to 3-12 months of the fees that a retailer has paid.
- The liability for any payment card brand fees is placed squarely on the retailer or is within this liability cap.
- No warranties or indemnities for data security or a breach thereof are included.
- The vendor is not contractually obligated to comply with the PCI DSS standard.
- Any custom code written to install the device or any custom interface between the retailer's system and the payment application is typically excluded from any PCI DSS warranty or contractual obligation. In fact, there are often express disclaimers from any PCI noncompliance or breach arising out of this custom code.

[2] You can find more information concerning the risks associated with class actions following data breaches in Bryan Cave's 2015 Data Breach Litigation Report.

Part II: Addressing Insurance Coverage Gaps

1. Do your existing policies cover data breaches?

Most retailers know they need insurance to cover traditional risks such as the possibility of fire, theft, or personal injury. Many retailers are not certain whether they need to purchase insurance to cover the risk of a data breach, and many assume that such risks are already covered by their existing insurance policies.

In analyzing whether your general insurance policies cover the risk of a data breach, retailers should consider the following:

- Several companies have argued that their losses from a data breach should be covered as "property damage" or "tangible property" under Commercial General Liability Policies ("CGL"). Most insurers take the position that standard CGL coverage items do not include data security; the result has been several high-profile coverage fights. The outcomes of those fights have been mixed. While some courts have sided with businesses, others have sided with insurers. *See, e.g., Acuity v. All-America Phillips Flower Shop,* 2914 WL 2740523 (Compl. Ill Cir. Ct.) (seeking declaratory action that "tangible property" does not include electronic data).

- Other companies have tried to argue that the disclosure of personal information as a result of a data breach constitutes "personal & advertising injury" under media liability policies. This too has led to coverage fights with mixed results.

- Insurance companies are trying to avoid these types of coverage fights by drafting explicit exclusions in most CGL and media policies that make clear that "cyber" events – including data breaches – are not covered, unless the insured has purchased a separate cyber policy or cyber endorsement. The result is that companies with more recently manuscripted policies are less able to argue that traditional CGL or media policies cover data security breaches.

2. Do you need cyber-insurance?

Recently, industry regulators and government agencies weighed in on the value to companies of insurance that is specifically designed to cover part, or all, of the costs of a data security breach ("cyber-insurance"). In September 2015, Deputy Treasury Secretary Sarah Raskin asked for the insurance industry to help protect against cyber threats.[3] In addition, the Securities and Exchange Commission (SEC) has started to focus on cybersecurity in its examination procedures, and examiners now gather information on

[3] Remarks by Deputy Secretary Sarah Bloom Raskin at The Center for Strategic and International Studies Strategic Technologies Program (Sept. 10, 2015).

cybersecurity controls – including specific information related to cyber-insurance and coverage.[4] While in 2014 only 31% of companies had purchased cyber-insurance,[5] the percentage has risen significantly due to a number of factors, such as the increased cost of data breaches, the higher number of insurance companies offering cyber-insurance policies, and the improved breadth of coverage available. In determining whether you need cyber-insurance, retailers should ask the following questions:

1. What are the first party costs that my organization would incur in the event of a typical data breach, and in the event of a catastrophic data breach?

2. Without insurance, would those first party costs pose a significant risk to my organization, our capital flow, or our earnings?

3. Does the cyber-insurance policy I am considering cover those first party costs?

4. What are the total third party costs that my organization would incur in the event of a typical data breach, and in the event of a catastrophic data breach?

5. Without insurance, would those third party costs pose a significant risk to my organization, our capital flow, or our earnings?

6. Does the cyber-insurance policy I am considering adequately cover the third party costs that we might incur?

7. Are any of our regulators adding cyber-insurance as a key factor in evaluating a company's cyber preparedness?

Look for variety in both coverage breadth and breach response service features.

The cyber-insurance market has evolved considerably, and there is much variety in both coverage breadth and breach response service features. McGriff cautions that companies should not be too quick to accept policy forms with sub-limits, stacking retentions, and limiting definitions/exclusions.

There are several markets, including many Lloyd's syndicates which will write policies with broad insuring agreements and without these drawbacks. This allows the Insured to deploy its coverage resources commensurate with the nature and scope of the breach event. Costs for forensic investigations, notification (statutory and voluntary), identity theft restoration services, regulatory investigations as well as PCI fines, penalties, and assessments (fraud costs + card reissuance fees) are very significant individually as well as collectively.

Answering these questions can be difficult. The first party and third party costs that an organization might incur can differ dramatically depending on the industry in which your organization operates, and the quantity of credit card transactions that your organization processes. Furthermore, cyber-insurance policies differ dramatically in terms of what they cover, what they exclude, and the amount of retentions (the amount of money for which the organization is responsible before the policy provides reimbursement to the organization).

[4] U.S. Securities and Exchange Commission, Office of Compliance Inspections and Examinations (OCIE) 2015 Cybersecurity Examination Initiative (Sept. 15, 2015).
[5] Ponemon Institute, 2014 Cost of Data Breach Study: Global Analysis at 22 (May 2014).

The following checklist can help guide the evaluation of a cyber-insurance policy to help determine if a policy is needed, and if the policy you are considering provides appropriate coverage, retention, and limits.

First Party Costs

Forensic Investigators

- **Coverage**: Does the policy cover the cost of retaining a forensic investigator? If so, are you limited to a single investigator, or are there situations in which the policy would permit you to hire multiple investigators – such as a PFI and a privileged forensic investigator – if needed?

- **Sub-limit**: Does the policy have a sub-limit for forensic investigation related costs? Is the sub-limit proportionate to the average cost of retaining a forensic consultant to investigate a data security incident? Would the sub-limit be sufficient if more than one forensic consultant must be retained?

- **Sub-Retention**: Does the policy have a sub-retention when hiring an investigator? If so, is the sub-retention well below the average cost of retaining a forensic investigator? If not, does the organization understand that the coverage will only provide protection for catastrophic incidents?

Even once a company enters into a cyber-insurance policy, it must continue to evaluate data security risks and to assess coverage accordingly. Saving a little in premium on the front-end can often lead to costly, uninsured, or underinsured expenses.

Outside Counsel

- **Coverage**: Does the policy permit you to retain an attorney to help your organization investigate and document a data security incident, retain investigators if needed, review contracts with service providers, identify statutory obligations to notify consumers and regulators, and advise your organization concerning steps that may reduce the likelihood of a class action or a regulatory investigation? Does the policy cover legal expenses incurred in defending all types of claims?

- **Exclusions**: Does the policy exclude coverage for lawyers to provide assistance concerning some aspect of a security breach response? For example, does the policy exclude coverage if your attorney attempts to negotiate or settle contractual claims, or has to deal with government regulators? Does the policy

exclude claims asserting legal theories that are common in class actions (consumer fraud or deceptive practices claims)?

- **Paneled providers**: Does the policy require that you use a specific law firm or does it provide a panel of law firms? Do you have relationships with any of the firms that are on the panel? If not, have you done due diligence concerning their experience in handling data security breaches and to verify that they do not have a conflict representing your company? Have you investigated whether the firm has taken legal positions that might benefit your insurer, but be inconsistent with your organization's ability to obtain coverage under your policy? Have the law firms that are recommended or required by the insurer agreed not to sue the insurer, on your behalf, to obtain coverage under your policy?

Crisis Management

- **Coverage**: Does the policy permit you to retain a public relations firm to help your organization plan for, or react to, news stories about the security breach? Does the policy exclude acts of terrorism or similar claims from coverage (state-sponsored hacking)? Does the policy address special needs your company may have based on your, or your vendor's, location of data storage?

- **Paneled providers**: Does the policy require that you use a specific public relations firm? Does that firm understand your company, your industry, and your clients? What other breaches has that firm handled? Do you think that those breaches were handled well or poorly from a public relations perspective?

Consumer Notifications

- **Coverage**: Does the policy cover the cost of issuing notices to consumers? If so, does the coverage give your organization the right to control how those notices are given (in paper format versus electronic format)? Does it require that your organization avail itself of "substitute notice" when permitted by statute? If so, does your organization understand that the policy may not pay for printing and mailing notification letters if your organization decides that issuing notifications in that manner is necessary to help protect the organization's reputation and brand?

- **Exclusions**: Does the policy exclude notifications that are not expressly required under a state data breach notification statute ("voluntary" notifications)? If so, are there situations in which your organization may decide to issue a voluntary notice in order to limit reputational damage or decrease the likelihood of a class action filing? Does your organization understand that these may not be covered under the policy?

- **Sub-limit**: Does the policy have a sub-limit for the total costs in issuing consumer notifications or the total number of consumer notices for which the policy will provide reimbursement? If so, is the sub-limit proportionate to the quantity of consumers about which the organization maintains personal information?

- **Sub-retention**: Does the policy have a sub-retention for either the cost of issuing consumer notifications or the number of consumer notices that must be paid for by the organization? If so, is the sub-retention well below the total quantity of consumers about which the organization maintains personal information?

Credit Monitoring Related Services

- **Coverage**: Does the policy cover the cost of providing credit monitoring (monitoring a consumer's credit report for suspicious activity), identity restoration services (helping a consumer restore their credit or close fraudulently opened accounts), and identity theft insurance (defending a consumer if a creditor attempts to collect upon a fraudulently opened account and reimbursing a consumer for any lost funds) to consumers who may be impacted by a breach? If your cyber-insurance policy is intended to cover a breach of employee health data in addition to a PCI data breach, note that credit monitoring services are of limited utility when personal health information is compromised. As a result, ID theft restoration services may be more useful to repair a victim's stolen/corrupted health record identity.

- **Exclusions**: Does the policy exclude credit-monitoring related services where providing them is not "required" by law? If so, given the fact that there are currently no statutes that require credit monitoring services to be offered, is anything of value really being provided to the company under the policy?

- **Paneled providers**: Does the policy require that you use a certain company to provide credit-monitoring related services? If so, does the organization have a relationship with a different provider? Does the provider that is listed on the panel have a history of consumer complaints? Does it have a history of alleged unfair or deceptive trade practices? Does the provider, or your insurer, indemnify the organization for any consumer complaints concerning credit monitoring services that you do offer?

- **Sub-limit**: Does the policy have a sub-limit for the total cost that it provides for credit monitoring? If so, is the sub-limit proportionate to the average cost of providing credit monitoring multiplied by the quantity of consumers about which the organization maintains personal information?

- **Sub-retention**: Does the policy have a sub-retention? If so, is it well below the average cost of providing credit monitoring multiplied by the quantity of consumers about which the organization maintains personal information?

Third Party Claims

Contractual Liabilities / Types of Data / Payment Card Brand Fees

- **Coverage**: Does the policy cover contractual liabilities that result from a data security breach? In particular, if your organization accepts credit cards, does the policy cover contractual liabilities that may be owed to your payment processor or merchant bank? These are sometimes referred to as Payment Card Industry ("PCI") fines or assessments. New policies typically contain "contractual liability" exclusions and must be endorsed/amended to carve-back coverage for claims associated with Merchant Services Agreements or they will be considered excluded.

Watch out for other problem language buried in policy definitions, especially if the definition of "Damages" is defined to exclude PCI fines, penalties, or assessments.

- **Exclusions**: Does the policy exclude any type of contractual liability such as PCI fines or contracts that your organization may have with end-use consumers? If the policy specifically defines "PCI" related fines or assessments, does that definition include all of the possible payment card brand fees that may be imposed or only a subset of those fees?

- **Sub-limit**: Does the policy have a sub-limit for the amount of assumed liability or payment card brand fees that are covered? If so, is the sub-limit proportionate to the quantity of payment brand fees that your organization might incur?

- **Sub-retention**: Does the policy have a sub-retention? If so, is it well below the average payment brand fees that may be incurred?

Regulatory Proceedings

- **Coverage**: Does the policy cover regulatory proceedings that may result from a breach? If so, does the coverage extend to legal fees incurred in a regulatory investigation or regulatory proceeding? Does it also cover the fines or civil penalties that may be assessed as a result of a proceeding? Will the insurance provider expand this coverage to include informal inquiries as well?

- **Exclusions**: Does the policy exclude investigations brought by agencies that are likely to investigate your organization? For example, if your organization is under the jurisdiction of the Federal Trade Commission ("FTC"), does the policy exclude investigations brought by the FTC? Does the policy exclude coverage for investigations brought by state regulators under certain types of state statutes (state consumer protection statutes or state unfair or deceptive trade practice statutes)? Depending on your industry, is coverage included for other regulatory investigations that might arise such as state PSC/PUC if your company is a utility or a cooperative?

- **Sub-limit**: Is the sub-limit proportionate to the average cost of defending a regulatory investigation and/or the average cost of the fines assessed to other organizations in your industry?

- **Sub-Retention**: Does the policy have a sub-retention for the cost of a regulatory investigation? If so, is the sub-retention well below the average cost of regulatory penalties and fines? If legal fees incurred in a regulatory investigation are covered, is the sub-limit well below the legal fees that you would expect?

Class Actions

- **Coverage**: Does the policy provide coverage for consumer claims that arise as a result of a credit card breach?

- **Exclusions**: Does the policy exclude any of the legal theories that consumers are likely to assert? Specifically, does it exclude coverage for assumed contractual liabilities, or allegations that the retailer was deceptive when describing its security practices, or that the retailer's actions relating to data security were "unfair?"

- **Sub-limit**: Is the sub-limit proportionate to the average cost of defending a class action and/or the average cost of the settlements that have occurred in your industry?

- **Sub-Retention**: Does the policy have a sub-retention for the cost of defending class actions?

Additional information concerning how to prepare for, and respond to, a data breach – including how to evaluate cyber-insurance – can be found within the *Data Security Breaches: Incident Preparedness and Response Handbook* published by the Washington Legal Foundation.

Authors

David Zetoony is the leader of Bryan Cave's global data privacy and security practice. He has extensive experience advising clients on how to comply with state and federal data privacy and data security laws. In addition, he has investigated hundreds of data security breaches, represented clients before the Federal Trade Commission, and defended national class actions. Contact David at (303) 417-8530 or david.zetoony@bryancave.com.

Courtney Stout has experience with a multitude of privacy and data security matters. Her practice focuses on the intersection between privacy, technology, and financial services. She advises clients on privacy and data security matters with a view toward identifying and minimizing risk from a potential data or cybersecurity incident, as well as regulatory compliance. Contact Courtney at (202) 973-4238 or courtneystout@dwt.com.

Suzanne A. Gladle, ARM is the director of cyber program operations at McGriff, Seibels & Williams, Inc. Suzanne has 28 years of risk and insurance experience having worked in various risk management capacities at Scientific-Atlanta, C&S Corporation (now Bank of America), and BellSouth Corporation where she oversaw the Executive Liability placement and administration for BellSouth's worldwide programs. She started with McGriff in 2000 and currently oversees operations for McGriff's expanding cyber resources. Contact Suzanne at (302) 239-2046 or sgladle@mcgriff.com.