AN A.S. PRATT PUBLICATION
MAY 2016
VOL. 2 • NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 2 | NUMBER 4 | MAY 2016

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3000
Fax Number .... (518) 487-3584
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3000

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [121] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2016–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

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

By David A. Zetoony and Courtney K. Stout*

In this first part of a two-part article, the authors assess the risk to a retailer from a credit card data breach. The second part of the article, which will appear in an upcoming issue of Pratt's Privacy & Cybersecurity Law Report*, addresses insurance coverage gaps.*

Most retailers do not realize that by accepting credit cards they expose themselves to the risk of a data security breach and significant potential costs and legal liabilities. This two-part article explains the key risks that a retailer faces following a data security breach of its payment card systems as well as the potential for addressing some of those risks through the purchase of cyber-insurance.

This first part of the article spells out the major sources of direct costs for retailers following a data breach. These costs often include retaining a payment card industry ("PCI") certified forensic investigator. Costs also typically include the retaining of a privileged forensic investigator (often by the retailer's law firm or general counsel); the hiring of outside counsel; public relations and crisis management; and consumer notification including printing and mailing costs and protection services offered to consumers.

In addition to the direct costs following a data breach, retailers often face three forms of liability from third parties: payment card brand fees; regulatory costs arising from investigations from the Federal Trade Commission ("FTC"), Securities and Exchange Commission ("SEC"), and State Attorneys General, for example; and class action exposure. Payments brands can assess more than 25 different contractual penalties, fines, adjustments, fees and charges upon a retailer following a PCI data security breach.

Contrary to what many retailers believe, retailers are typically not shielded from liability by their card processor or device manufacturers in the event of a payment card data breach. The "fine print" in the contracts for these products or services usually includes a number of provisions that place the liability on the retailer.

---

* David A. Zetoony, a partner at Bryan Cave LLP and the leader of the firm's global data privacy and security practice, advises clients on how to comply with state and federal privacy, security, and advertising laws, represents clients before the Federal Trade Commission, and defends national class actions. He may be contacted at david.zetoony@bryancave.com. Courtney K. Stout is counsel at Davis Wright Tremaine LLP, where she is a privacy and security attorney advising clients in the technology, data security, and financial services industries. She may be contacted at courtneystout@dwt.com. Suzanne Gladle, ARM, the director of Cyber Program Operations at McGriff, Seibels & Williams, Inc., contributed to this article. She may be contacted at sgladle@mcgriff.com.

The second part of the article, which will appear in an upcoming issue of *Pratt's Privacy & Cybersecurity Law Report*, provides readers with a checklist to help them evaluate whether a cyber-insurance policy is needed, and if the policy they are considering provides appropriate coverage, retention and limits in light of the costs detailed earlier.

ASSESSING THE RISK TO A RETAILER FROM A CREDIT CARD DATA BREACH

One source estimates that 60 percent 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 are exposed to the risk of a data security breach and substantial potential costs and legal liabilities. This section explains the key risks that a retailer faces following a data security breach of their payment card systems.

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 fees.

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.

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

Outside Counsel

Outside counsel is typically needed to negotiate agreements between the retailer, the PFI, and the privileged forensic investigator. Outside counsel also 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.

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 article as "fees," the following provides an example of the different categories of penalties that can be imposed by just one payment brand:

- 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; and
- 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.

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 percent of publicly reported breaches relate to the retail industry, nearly 80 percent 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.

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 three to 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.

***

The second part of this article will appear in an upcoming issue of *Pratt's Privacy & Cybersecurity Law Report*.

Three Myths – and the Facts

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).

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.

Myth: Every data breach results in a class action.

Fact: Most data breaches do not result in litigation. In fact, only four percent 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.