AN A.S. PRATT PUBLICATION
JUNE 2016
VOL. 2 • NO. 5

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 2 | NUMBER 5 | JUNE 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 [153] (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 II

By David A. Zetoony and Courtney K. Stout*

In the first part of this two-part article, which appeared in the May 2016 issue of Pratt's Privacy & Cybersecurity Law Report*, the authors assessed the risk to a retailer from a credit card data breach. This second part of the article addresses insurance coverage gaps.*

ADDRESSING INSURANCE COVERAGE GAPS

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.[1]
- 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

* 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.

[1] *See, e.g., Acuity v. All-America Phillips Flower Shop*, Compl. Ill Cir. Ct., (seeking declaratory action that "tangible property" does not include electronic data).

result is that companies with more recently manuscripted policies are less able to argue that traditional CGL or media policies cover data security breaches.

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.[2] In addition, the Securities and Exchange Commission ("SEC") has started to focus on cybersecurity in its examination procedures, and examiners now gather information on cybersecurity controls – including specific information related to cyber-insurance and coverage.[3] While in 2014 only 31 percent of companies had purchased cyber-insurance,[4] 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?

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

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

[3] U.S. Securities and Exchange Commission, Office of Compliance Inspections and Examinations (OCIE) 2015 Cybersecurity Examination Initiative (Sept. 15, 2015).

[4] Ponemon Institute, 2014 Cost of Data Breach Study: Global Analysis at 22 (May 2014).

amount of money for which the organization is responsible before the policy provides reimbursement to the organization).

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?

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.

- **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?

CONCLUSION

- 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. 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.
- 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 frontend can often lead to costly, uninsured, or underinsured expenses.
- Watch out for problem language buried in policy definitions, especially if the definition of "Damages" is defined to exclude PCI fines, penalties, or assessments.

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.[5]

[5] http://www.wlf.org/upload/legalstudies/monograph/ValdeteroZetoonyFinal.pdf.