AN A.S. PRATT PUBLICATION
NOVEMBER – DECEMBER 2017
VOL. 3 • NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 NUMBER 9 NOVEMBER/DECEMBER 2017

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) 487-3385
Fax Number .... (800) 828-8341
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 ..... (937) 247-0293

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 [303] (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

(2017–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.

Cyberattacks Are the New Norm: How to Respond and Get Insurance Recovery for Government Investigations

By Joseph D. Jean, Carolina A. Fornos, and Brian E. Finch*

Companies that suffer cyberattacks can expect not sympathy but scrutiny from legal authorities. The authors of this article discuss how strategic negotiation of directors and officers, errors and omissions, and cyber insurance policy language can cover not only litigation but also investigation costs and help to mitigate any cyber claims that may arise.

The script is well-worn by now: a major corporation suffers an embarrassing data breach that has led to the loss of tens of millions of customer records. Compounding the embarrassment is the quick reaction by state attorneys general ("AG") launching investigations and lawsuits against the corporation and executives. Cyber policies are the obvious first line of defense. But will your directors and officers ("D&O") liability insurance and errors and omissions ("E&O") insurance carriers help cover the costs associated with defending against the AGs' claims?

BACKGROUND: STATE AGS ARE AGGRESSIVELY USING THEIR AUTHORITY UNDER DATA PRIVACY AND UNFAIR/DECEPTIVE ADVERTISING LAWS TO PURSUE CLAIMS FOLLOWING CYBERATTACKS

The last 10 years have seen an explosive growth in the number of data privacy protection laws enacted and updated across the country. Nearly every state now has a law requiring companies of all shapes and sizes to disclose when "personally identifiable information" (or "PII," a term whose meaning varies from state, but typically involves some combination of a person's name and a unique identifier like a social security number, credit card or other payment account number, or driver's license number) has either been accessed without authorization or stolen.

Under those laws, companies will have a set amount of time to notify affected individuals as well as provide them some form of recourse, typically through free access to credit monitoring services. Additionally, the data privacy protection laws

* Joseph D. Jean, a Pillsbury Winthrop Shaw Pittman LLP partner and trial lawyer, advocates for commercial insurance policyholders against their insurance companies. Carolina A. Fornos, a litigation partner at the firm is a trial and appellate attorney whose practice areas include commercial litigation, civil and criminal enforcement matters, and cross-border internal investigations and compliance. Brian E. Finch, a public policy partner at the firm, provides legal counsel to companies regarding regulatory issues, cyberattacks, national defense and intelligence policies, and homeland security concerns. The authors may be contacted at joseph.jean@pillsburylaw.com, carolina.fornos@pillsburylaw.com, and brian.finch@pillsburylaw.com, respectively.

also usually give an individual attorney general the authority to pursue litigation against the companies whose databases were stolen. Such actions initially were only taken following the most egregious data breaches (extremely large size or the security failure appeared to have been the result of gross negligence on the part of the company.) Now, however, attorneys general are increasingly filing such lawsuits simply upon receipt of news that a data breach has occurred. Most troublesome for some companies is that they might be sued before they even know how the breach occurred or who conducted it.

Such investigations tend to be expensive, protracted, and disruptive to the company's efforts to conduct day-to-day business. Executives and officers often find themselves being deposed by multiple attorneys general offices as well as civil plaintiffs while simultaneously being excoriated in the press for their alleged malfeasance or perceived lack of interest in protecting the data of their customers. Even though a determination as to whose actions were ultimately responsible the cyberattack may be months or even years away—and may require the resources of federal law enforcement and national security agencies to make a definitive conclusion—the costs of internal investigations, settlement negotiations or even lawsuits can seriously impair the day-to-day operations of a company.

STRATEGIES FOR MANAGING AND RESPONDING TO CIVIL INVESTIGATIVE DEMANDS AND SUBPOENAS

In the event of a cyberattack, a company can anticipate Civil Investigative Demands ("CIDs") or subpoenas will be issued. How the company responds will be critical. The company should review the subpoena, Civil Investigative Demand, other investigative demand or lawsuit carefully to ensure that it understands the scope of information requested, terms used, and time frame affected. It is highly advised that counsel experienced in handling government investigations be consulted.

Counsel can begin the conversation with the issuing government official in order to respond properly to the information being requested by the government. Counsel can help to evaluate whether the scope of the request may be narrowed to (i) effectively target the relevant information sought by the government, and (ii) efficiently respond to the government's requests and minimize the disruption that collecting such information entails.

Counsel can also advise on the potential for working with the government to identify the culprit of the cyberattack. These initial discussions will greatly impact the government's perception of the situation and how it treats the company throughout the investigation. Moreover, it is highly likely that the company will want to conduct an internal investigation to address potential risks and liabilities that may flow from the government request.

INSURANCE COVERAGE FOR DATA BREACH/CYBERSECURITY INVESTIGATIONS

Targets of cyber-related attacks can expect to incur significant expenses if they are forced to respond to government investigations into a data breach. The categories of costs faced by the subject of such an investigation (apart from the costs associated with the breach itself and the resultant lawsuits) could include:

- Outside counsel fees for the review of a subpoena, CID or other information request, and for the review and production of documents;
- The cost of any internal investigation commissioned by the company;
- Outside counsel fees for ongoing interaction with the AG or other enforcement officials; and
- Settlements or judgments associated with the investigation or resulting lawsuits.

In addition, publicized government scrutiny of a data breach could inspire civil actions such as shareholder derivative suits and securities class actions and lawsuits by individuals whose PII was stolen.

Fortunately, companies should be able to call upon their cyber policies to provide coverage.[1] But directors and officers and possibly other liability insurers, which may be overlooked in situations like this, should also line up to help defray these costs. D&O policies, for example, cover "claims" arising from alleged "wrongful acts" of certain officers, directors, and employees of the company, as well as, in some cases, those of the company itself. Depending upon the wording of each particular policy, investigation-related expenses may be covered. Potential sources of recovery should not be overlooked simply because an insurer or broker asserts that the "conventional wisdom" is that a certain policy is not "meant" to cover subpoenas or other investigation response costs. Third-party vendors may also owe indemnification to companies who have been the victim of a data breach and, in some cases, may also have named such companies as additional insureds on certain liability policies. Be sure to investigate all potential sources of recovery.

GETTING COVERAGE FOR SUBPOENA RESPONSE COSTS UNDER A D&O POLICY

The subpoena—a written order commanding the production of documents and/or witness testimony—is a widely used tool in government investigations, and is often the first step in a larger investigation. As a threshold matter, insurers often dispute that a

[1] Because many cyber policies specifically cover government investigations, they are the obvious first line of defense. But even today, many companies do not have cyber policies and even those that do may not have sufficient limits to cover the entirety of the event. That is why this article focuses on D&O and E&O policies, which may be available to provide valuable coverage.

subpoena is a "claim" within the meaning of that term in D&O policies. There is an emerging consensus in various jurisdictions that insurers are wrong on this issue.

The typical D&O policy contains a definition of "claim" similar to the following:

(1) a written demand for monetary or nonmonetary relief;
(2) a civil, criminal, administrative, regulatory or arbitration proceeding for monetary or nonmonetary relief which is commenced by:
    (i) service of a complaint or similar pleading;
    (ii) return of an indictment, information, or similar document (in the case of a criminal proceeding); or
    (iii) receipt or filing of a notice of charges.

A number of courts have held that a subpoena constitutes a "demand for nonmonetary relief."

An important recent New York case is *Syracuse University v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.*, in which the New York Supreme Court, affirmed by the Appellate Division, held that under the policy's definition of "claim," the plain meaning of the term "nonmonetary relief" encompassed subpoenas issued by the U.S. Attorney's Office and a county district attorney's office in connection with their investigations into sexual abuse. The court relied heavily on *MBIA Inc. v. Federal Ins. Co.*, in which the U.S. Court of Appeals for the Second Circuit found coverage for subpoena response costs, stating: "We reject the insurers' crabbed view of a subpoena as a 'mere discovery device' that is not even 'similar' to an investigative order. New York case law makes it crystalline that a subpoena is the primary investigative implement in the NYAG's toolshed." The *Syracuse University* court also noted that, pursuant to both New York and federal law, failure to comply with a subpoena is a punishable offense. Courts in other jurisdictions also have found D&O coverage for subpoena response costs.[2]

Courts have also found coverage under errors and omissions policies for subpoenas and CIDs. For example, *Ace American Insurance Co. v. Ascend One Corp*. involved a policyholder that was subject to an administrative subpoena issued by the Maryland Attorney General's office and a CID issued by the Texas Attorney General's office. The E&O policy at issue defined "claim" to include "[a] civil, administrative or regulatory investigation . . . commenced by the filing of a notice of charges, investigative order or similar document." Applying Maryland law, the U.S. District Court for the District of

[2] *Protection Strategies v. Starr Indem. and Liab. Co*. (E.D. Va.) (applying Virginia law and finding defense coverage for NASA subpoena and search and seizure warrant); *Minuteman International Inc. v. Great American Ins. Co*. (N.D. Ill.) (applying Illinois law and finding coverage for compliance with SEC subpoena); *Polychron v. Crum & Forster Ins. Cos*. (8th Cir.) (applying Arkansas law and finding coverage for grand jury subpoena served on a bank).

Maryland held that the subpoena and CID were part of an investigation into potential consumer protection law violations, and were therefore an "investigation" under the policy.

COVERAGE FOR OTHER INVESTIGATION-RELATED COSTS

In addition to responding to a subpoena, companies facing an AG investigation may engage in many other costly tasks. For example, in some cases, a subpoena may be preceded by a less formal information request from the authorities, and decisions will have to be made (often with the advice of outside counsel) as to whether and how to respond to such requests. In the *MBIA* case mentioned above, the Second Circuit found coverage for costs incurred by the insured in voluntarily complying with the Securities and Exchange Commission's and New York AG's informal, oral document requests. The Second Circuit held that this activity was covered because it was intended to head off formal subpoenas and additional public relations damage.

A company under investigation may also engage a public relations firm, security service and other vendors to help manage the fallout from publicized government scrutiny. While these "indirect" response costs are arguably investigation defense costs, there is scant case law on whether they are covered. But a policy with "crisis response" coverage might provide some relief. Coverage might also be available for resulting shareholder lawsuits, because such lawsuits commonly fit into the definitions of "claim" in D&O and E&O policies.

PRACTICAL TIPS FOR POLICYHOLDERS

Companies should keep the following points in mind in order to maximize coverage for government investigations:

- Be proactive. Even before a subpoena or "target letter" lands on the general counsel's desk, work with your broker to negotiate broad coverage under a robust cyber program.
- Consider all policies. Also negotiate a relatively broad definition of "claim" in your D&O and E&O policies. Some newer policy language can provide coverage for certain "pre-claim" inquiries from government agencies and specifically for subpoenas, which would also include attorneys' fees and costs associated with interviews or meetings with enforcement authorities. Policy exclusions must also be scrutinized. Consult competent coverage counsel to review proposed policy language.
- Understand and comply with notice obligations. A government investigation may begin with a formal subpoena, or even informally at an earlier point in time. It is essential that you understand when, under your policies, notice of claim, or notice of circumstances giving rise to a claim, must be given. On a

similar note, it is important to understand your obligation to provide information to and cooperate with your insurer in defending an investigation. Best practice is to involve coverage counsel early—the advice will be protected by the attorney-client privilege, whereas conversations with a broker may not be.

When faced with a government investigation, policyholders should carefully examine all potentially available sources of coverage. The law is different in many states, and some courts have not addressed the issue. Policyholders should be careful to understand their policies, the law, and their risks before they are subject to an investigation.