Financial Fraud Law Report

AN A.S. PRATT & SONS PUBLICATION **JULY/AUGUST 2014**

LexisNexis

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:
Catherine Dillon at 908-673-1531
Email: ..... catherine.dillon@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

Library of Congress Card Number: 80-68780

ISBN: 978-0-7698-7816-4 (print)
ISBN: 978-0-7698-7958-1 (eBook)

Cite this publication as:

Financial Fraud Law Report § [sec. no.] (LexisNexis A.S. Pratt);
Financial Fraud Law Report § 1.01 (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

An A.S. Pratt™ Publication

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

MATTHEW BENDER

(2014–Pub.4759)

Editor-in-Chief & Board of Editors

Matthew Bender, 121 Chanlon Road, North Building, New Providence, NJ 07974. Direct inquiries for editorial department to catherine. dillon@lexisnexis.com. *ISBN: 978-0-76987-816-4*

Data Breach Law: A Shifting Landscape

By Michael G. Morgan, Jessica M. Sawyer, and Eli A. Alcaraz*

This article surveys recent data breach developments, including changes in the types of attacks that most commonly result in breaches and developments in the legal obligations regarding data security and notification to consumers and law enforcement after a breach. In addition, the authors reiterate the key recommendations for responding to a breach.

Introduction

You have seen the names in the news: eBay, Target, AT&T, even the University of Maryland. The publicity surrounding recent data breaches has focused the public's attention more than ever on the risks to consumers and has raised public concerns over data security and privacy. Against this backdrop, this article surveys recent data breach developments, including changes in the types of attacks that most commonly result in breaches and developments in the legal obligations regarding data security and notification to consumers and law enforcement after a breach. Finally, the article reiterates the key recommendations for responding to a breach.

Evolving Data Security Threats

One cause of the increased public attention to data breaches is that the character of the breaches has shifted from geopolitical attacks, such as the Red October cyber-espionage campaign, to large-scale attacks on the payment card systems of major retailers and other businesses.[1] Most of these attacks are point-of-sale intrusions, such as the installation of malware to collect magnetic stripe data, and web application attacks that steal payment card information or financial credentials like usernames and passwords.[2] Others exploit security vulnerabilities, such as the "Heartbleed bug," which exposed the encryption keys on which millions of users relied to protect their online information, including email addresses, usernames, passwords and financial account numbers. Other explanations for the increased public attention include the volume of breaches (an estimated 1,367 confirmed data breaches and 63,437 security incidents occurred worldwide last year[3]) and the flurry of publicity about the breaches, which often focuses more on the number of records

---

* Michael G. Morgan (mgmorgan@jonesday.com) is of counsel in the Business and Tort Litigation group at Jones Day in its Los Angeles office and is a Certified Information Privacy Professional by the International Association of Privacy Professionals. Jessica M. Sawyer (jsawyer@jonesday.com) and Eli A. Alcaraz (ealcaraz@jonesday.com) are associates at the firm. The authors acknowledge and thank Kelly Ozurovich, a summer associate at the firm, her help and contribution to this article.

[1] Verizon 2014 Data Breach Investigations Report, at 3, *available at* http://www.verizonenterprise.com/DBIR/2014/.

[2] Verizon 2014 Data Breach Investigations Report, at 16, 20, *available at* http://www.verizonenterprise.com/DBIR/2014/.

[3] Verizon 2014 Data Breach Investigations Report, at 2, *available at* http://www.verizonenterprise.com/DBIR/2014/.

that were compromised than whether consumers actually have been harmed or exposed to any genuine risks.

Notwithstanding the increased concern, many consumers appear quite willing to share personal information with retailers and other companies, if they think they will benefit.[4] But while consumers are willing to allow companies access to their data, they expect some increased security in return. Eighty-two percent of the respondents in a recent study expect their banks to use data analysis to protect against fraud, and 76 percent would consider switching to a competitor which could offer assurances that their financial information would be safer.[5]

In response to data breaches, companies are developing or refining their breach response plans, hiring security experts and privacy counsel, offering free credit monitoring to persons whose information has been compromised,[6] and taking advantage of insurance policies to cover potential online attacks. The insurance policies typically cover immediate costs, such as cleanup, notification, and credit monitoring.[7] Unfortunately, they do not necessarily cover litigation or the costs of reputational damage.

Evolving Data Security Obligations

Although companies can easily identify the data security obligations they have voluntarily assumed in contracts or privacy policies, it can often be more difficult to identify the obligations arising under the law. There is no overriding federal data security law; rather, the obligations often need to be discerned from federal enforcement actions, such as the FTC's high-profile action against Wyndham Hotels.

Several years ago, Wyndham suffered three data breaches by hackers with domain addresses registered in Russia.[8] The FTC sued Wyndham in early 2012 under Section 5 of the Federal Trade Commission Act, which prohibits "unfair acts or practices." In essence, the FTC asserts that its authority to act against "unfair" practices allows it to

---

[4] "To me this is all about competition and in this case [the company] is doing its best to give you the products you need most. As a software engineer and technology enthusiast I'm happy to see companies doing all they can to make my experience easier and less time consuming." Kashmir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, FORBES, Comment of Tom Petracca, *available at* http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/, (last visited Jan. 16, 2014, 11:41 AM).

[5] Ayaz Nanji, *When Consumers Will (and Won't) Share Personal Data [Infographic]*, MARKETINGPROFS, *available at* http://www.marketingprofs.com/charts/2013/11512/when-consumers-will-and-wont-share-personal-data-infographic, (last visited Jan. 16, 2014, 11:48 AM).

[6] Matt Wilson, *Target, Neiman Marcus scramble to ally data breach worries*, PRDAILY.COM, *available at* http://www.prdaily.com/Main/Articles/Target_Neiman_Marcus_scramble_to_allay_data_breach_15911.aspx (last visited June 16, 2014, 10:35 AM).

[7] Nicole Perlroth & Elizabeth A. Harris, *Cyberattack Insurance a Challenge for Business*, NEW YORK TIMES, *available at* http://www.nytimes.com/2014/06/09/business/cyberattack-insurance-a-challenge-for-business.html?_r=0, (last visited June 16, 2014, 11:32 AM).

[8] Elinor Mills, *FTC sues Wyndham hotels over data breaches*, CNET.COM, *available at* http://www.cnet.com/news/ftc-sues-wyndham-hotels-over-data-breaches/, (last visited June 13, 2014, 1:41 PM).

take action against companies with inadequate data security practices.[9] It also reveals what the FTC considers inadequate security. In particular, the FTC takes issue with such alleged practices as (1) failing to use firewalls to limit access to Wyndham's systems, (2) storing payment information in readable text, (3) failing to remedy known vulnerabilities on servers, such as the inability to receive security updates or patches, (4) failing to require user IDs and passwords that are difficult for hackers to guess, (5) failing to adequately inventory computers connected to its network, and (6) failing to follow proper incident response procedures.[10] The U.S. District Court for the District of New Jersey recently denied Wyndham's motion to dismiss, allowing the case to proceed.

Additionally, the FTC has had some success in forcing companies to take corrective actions as part of settlements of FTC claims for, among other things, allegedly inadequate security measures to protect Social Security numbers and credit and debit card numbers[11] and sensitive patient personal health information.[12] There also has been class action litigation relating to data breaches. Although these cases traditionally have been challenging for plaintiffs, largely because of the difficulty of proving actual harm to the class from the breach, there have been a number of recent, and costly, class action settlements in such cases.[13]

Data Breach Notification Laws

There is no federal standard for notification in the wake of data breach. This lack of a federal standard is noted in the May 2014 White House Report on Big Data.[14] The Report recommends that "Congress should pass legislation that provides for a single national data breach standard along the lines of the Administration's May 2011

---

[9] First Amended Complaint, *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf.

[10] First Amended Complaint, ¶ 24, *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf.

[11] *Cord Blood Bank Settles FTC Charges that it Failed to Protect Consumers Sensitive Personal Information*, Federal Trade Commission, *available at* http://www.ftc.gov/news-events/press-releases/2013/01/cord-blood-bank-settles-ftc-charges-it-failed-protect-consumers, (last visited June 16, 2014, 12:23 PM).

[12] *Accretive Health Settles FTC Charges That It Failed to Adequately Protect Consumers' Personal Information*, Federal Trade Commission, *available at* http://www.ftc.gov/news-events/press-releases/2013/12/accretive-health-settles-ftc-charges-it-failed-adequately-protect (last visited June 16, 2014, 12:29 PM).

[13] *See, e.g.*, Jaikumar Vijayan, *TJX reaches $9.75 million breach settlement with 41 states*, COMPUTERWORLD.COM, http://www.computerworld.com/s/article/9134765/TJX_reaches_9.75_million_breach_settlement_with_41_states (last visited June 13, 2014, 2:50 PM); Marianne Kolbasuk McGee, *Settlement in AvMed Breach Suit: Class Action Settlement Offers Payments for Lack of Security*, DATABREACHTODAY.COM, http://www.databreachtoday.com/settlement-in-avmed-breach-suit-a-6188 (last visited June 13, 2014, 2:41 PM).

[14] *Big Data: Seizing Opportunities, Preserving Values*, Executive Office of the President, *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf (May 1, 2014).

Cybersecurity legislative proposal."[15] The Report suggests that "[s]uch legislation should impose reasonable time periods for notification, minimize interference with law enforcement investigations, and potentially prioritize notification about large, damaging incidents over less significant incidents."[16]

The Report's recommendations are not law and, unless and until there is an overriding federal standard, companies will need to consider the many state laws in this area. Currently, laws in forty-seven states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands require companies to notify individuals of data breach involving personally identifiable information. The three states without such laws are Alabama, New Mexico, and South Dakota.

Data Breach Response: 6 Key Steps[17]

Introduction

Although each data breach presents its own challenges, six key steps should be taken in response to a breach.

Step 1. Prepare and Practice

No matter how secure your systems, or how minor the types of data you collect, you should prepare for a data breach by assuming it will happen. To prepare for a breach, assemble a breach response team that will coordinate the company's response to breaches. The team should include employees from all areas of the company, from legal, compliance, information technology, public relations, and customer service, and should include an in-house lawyer or outside counsel with expertise on data breach and privacy issues. To prepare for a breach, consider running practice drills through simulated data breaches. As soon as a breach is detected, immediately notify the internal response team. Communication will be critical, so this team will take the lead on making sure that both internal stakeholders and outside services, such as privacy counsel, are kept in the loop. The team should be integrated across the

---

[15] *Big Data: Seizing Opportunities, Preserving Values*, Executive Office of the President, at 62, *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf (May 1, 2014).

[16] *Big Data: Seizing Opportunities, Preserving Values*, Executive Office of the President, at 62, *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf (May 1, 2014).

[17] Compiled from Chris Preismesberger, *Data Breaches: 10 Common Mistakes That Put Enterprises at Risk*, EWEEK, *available at* http://www.eweek.com/security/slideshows/data-breaches-10-common-mistakes-that-put-enterprises-at-risk.html, (last visited Jan. 16, 2014, 12:05 PM); *Common data breach handling mistakes*, HELP NET SECURITY, *available at* http://www.net-security.org/secworld.php?id=15681, (last visited Jan. 16, 2014, 12:06 PM); *Data Breach Response Guide*, Experian, *available at* http://www.experian.com/assets/data-breach/brochures/response-guide.pdf; *If Customer Data is Stolen or Lost-What to Do Next*, Better Business Bureau, *available at* http://www.bbb.org/data-security/what-to-do-if-consumer-data-is-stolen/checklists/; Jeff Goldman, *How to Respond to a Data Breach, ESECURITY PLANT, available at* http://www.esecurityplanet.com/network-security/how-to-respond-to-a-data-breach.html, (last visited Jan. 16, 2014, 12:07 PM); *Responding to a Data Breach: Communications Guidelines for Merchants*, Visa, *available at* http://usa.visa.com/download/merchants/cisp_responding_to_a_data_breach.pdf.

company, allowing information about the breach to get to those who need it quickly and efficiently, without confusion or misinformation.

Step 2. Contain and Document

When a breach is identified, the internal response team, and particularly its information technology members, must act immediately to contain the breach and prevent additional damage. Containing the data breach is critical. Then, begin the process of documentation and analysis. You should make it a priority to thoroughly investigate and understand the breach, including the risks to consumers whose information may have been compromised. Not only will you need specific information in order to fulfill legal and regulatory obligations and take steps to prevent future breaches, but you will need to fully document and analyze your response to the breach.

Step 3. Report

The lawyers and other legal professionals on your data response team should prepare a plan to identify and meet all legal and regulatory obligations arising from the breach. Depending on the size and type of the breach, you may be required to report it to state or federal government agencies and consumer reporting agencies. You may also want to involve law enforcement, regardless of whether you have an obligation to report. Reporting information should be part of your breach response plan, so that you can meet the often quite tight reporting deadlines.

Step 4. Notify

Notification requirements are determined by the residence of the consumers whose information was compromised, not the location of your business. You will need to notify consumers in fairly short timeframes (some as short as 30-45 days), and preparation will be key. You should already have a basic notification template created as part of your data response plan, and should tailor it to your specific situation. This is where a standing contract with a data breach notification service may serve you well.

Step 5. Monitor and Update

Investigating the breach will take time. Convene regular meetings of the breach response team and make sure that updates go out regularly the internal response team and the public. Make sure that customer-facing employees are kept up-to-date and are able to give consumers accurate information and directions.

Step 6. Be Transparent

If the breach is large enough, you will not be able to avoid public scrutiny. Even smaller breaches may come to the attention of specific sectors. You do not want to be the company that publicly dismisses security concerns, only to have a breach made public by the media or persons whose information has been compromised. Instead, make sure that information about the breach and your response is coming from the company. This will allow you to explain the steps you are taking to address the breach. Transparency and honesty may allow your company to maintain (or later regain) the trust of your consumers. You should make sure that information is

available to consumers through multiple avenues. Consider creating web pages to disseminate information, and link them to the pages your consumers frequently access, and provide information in stores and through call centers. Consider partnering with a leading consumer reporting agency (e.g., Experian) to provide access to credit reports or credit protection services.[18] Create goodwill by treating the breach seriously and addressing consumer concerns.

---

[18] *Data Breach Response Guide*, Experian, *available at* http://www.experian.com/assets/data-breach/brochures/response-guide.pdf.