Skadden

Privacy & Cybersecurity Update

2017 Data Breach Incidents Hit New Record High

The Identity Theft Resource Center reported a record rise in reported data breach incidents in 2017.

Data breaches in the United States hit a new record high in 2017, according to the 2017 Data Breach Year-End Review (review) jointly released by the Identity Theft Resource Center (ITRC), a nonprofit organization that supports victims of identity theft, and CyberScout, a provider of data management and data security services.[1] The review states there were 1,579 such incidents in 2017, a record-breaking and dramatic increase of 44.7 percent over 2016.

Significantly, the number of data breaches represented in the review do not even reflect every U.S. data breach that occurred in 2017; rather, the count is based only on the number of data breach notifications that companies were legally required to report to state authorities or affected consumers. With multiple large, established companies facing public data breaches in 2017, the ITRC has suggested that the increase in identified data breaches is partly a result of industries' increased disclosure of data breaches affecting consumers.

Industries Affected

The review identified the top five industry sectors that were hit hardest by data breach incidents in 2017, with the percentage of breaches suffered by each:

1. Business: 55 percent
2. Medical/Health care: 23.7 percent
3. Banking/Credit/Financial: 8.5 percent
4. Education: 8 percent
5. Government/Military: 4.7 percent

[1] A copy of the review can be found here.

This was the third year in a row that the business sector topped the ITRC's Data Breach List, with the 55 percent the industry recorded representing 870 reported incidents in 2017. For the banking sector, this is only the second time since 2005 that it has been included in the top three of most affected industry sectors.

Methods of Exposure

The review tracks seven different ways in which a data breach may occur as a means of gauging the potential level of harm associated with a given data breach. These methods include: hacking (with subcategories of phishing, ransomware/malware and skimming); unauthorized access; insider theft; data on the move; accidental exposure; employee error, negligence or improper disposal/loss; and physical theft. According to the 2017 figures, hacking continues to rank the highest and was associated with approximately 59 percent of 2017 data breaches, with 21 percent of those breaches attributable to phishing. Below is an overall breakdown of how consumer information was exposed in 2017:

- Hacking: 59.5 percent, including phishing, malware/ransomware and skimming
- Unauthorized access: 10.8 percent (which, according to the ITRC, involves some kind of access to data but does not explicitly include the term hacking in publicly available breach notification letters)
- Employee error, negligence or improper disposal/loss: 10.4 percent
- Subcontractor, third party or business associate: 7.5 percent
- Accidental exposure: 6.4 percent
- Insider theft: 5.3 percent
- Physical theft: 4.5 percent
- Data on the move: 2.2 percent

Types of Data Exposed

Of the 179 million consumer records exposed last year, the review reported that nearly 158 million were Social Security numbers. Despite continuing debates among industry stakeholders on the utility of Social Security numbers as authenticators, it is clear that many companies continue to collect and process this information. In addition to increasing exposure of Social Security numbers, payment card data also saw rising vulnerability in 2017. Credit and debit card information accounted for nearly 20 percent of records exposed in 2017 (up from 6 percent of consumer records in 2016). The review notes that the actual number of records affected as reported in data breach notifications grew by 88 percent compared to 2016 figures; however, the review noted that only 37 percent of data breach notifications quantify the number of records exposed.

Key Takeaways

The review highlights that cybersecurity incidents are significantly increasing, further heightening the need for companies to have cybersecurity incident response plans in place and to ensure that cybersecurity risks are seen as enterprise-wide issues.

Return to Table of Contents

Supreme Court Allows Circuit Split on *Spokeo*'s Effects in Data Breach Cases to Continue

On February 20, 2018, the United States Supreme Court denied without comment the defendant insurer's petition for *certiorari* in *CareFirst, Inc. v. Attias*.[2] The Court's denial means the deepening divide between the circuit courts over what plaintiffs must allege to satisfy *Spokeo, Inc. v. Robins*[3] will continue.

Background

The lawsuit in *CareFirst, Inc.* arose after hackers breached a CareFirst database containing its policyholders' personal information. The allegedly unencrypted data included names, birthdays, email addresses, Social Security numbers and credit card information. Applying *Spokeo*, which requires that the "injury in fact" alleged in the complaint must be "concrete, particularized, and … 'actual or imminent' rather than speculative," the district court found that the increased risk of identity theft due to the breach alleged in the complaint was not "actual or imminent" and dismissed the case.

On appeal, a unanimous three-judge D.C. Circuit panel reinstated the class action, finding that the plaintiffs' allegation of a substantial risk of identity theft stemming from the breach was sufficient to confer standing.[4] The circuit court concluded that the district court erred in its interpretation of *Spokeo* and noted that, according to guidance under *Clapper v. Amnesty International USA*,[5] an injury may be sufficiently imminent when there is a "substantial risk" that it will happen.

[2] 583 U.S. __ (February 20, 2018).
[3] 578 U.S. __, 136 S.Ct. 1540 (2016).
[4] 865 F.3d 620, 629-630 (D.C. Cir. 2017).
[5] 568 U.S. 398 (2013).

Circuit Split

The decision in *CareFirst* aligned with decisions by the Sixth and Seventh Circuits, which have held that the risk of future harm may provide standing in data breach cases. In *Galaria v. Nationwide Mut. Ins. Co*.,[6] for example, the Sixth Circuit held although it was not certain that the plaintiffs would suffer an injury as a result of the theft of their data, there was a substantial risk of harm such that incurring mitigation costs was reasonable.[7] The court therefore held the plaintiffs had standing to pursue their case.

Conversely, the Second, Fourth and Eighth Circuits have each held the risk of potential future identity theft too remote to grant Article III standing. In *In re Supervalue, Inc*., *Consumer Data Security Breach Litigation*,[8] the Eighth Circuit held that the mere theft of credit card information without more — such as actual evidence of fraudulent charges — did not create a case or controversy under Article III. Similarly, in *Beck v. McDonald*,[9] the Fourth Circuit held that the threat of identity theft from a breach at a hospital was too speculative to constitute an injury in fact.

Key Takeaways

One possible explanation for the Court's denial of *certiorari* despite the circuit split is the factual discrepancies among the cases. While some cases have involved credit card information alone, others have involved a wider range of information.

The Supreme Court's refusal to address the current circuit split means continuing uncertainty for plaintiffs and defendants alike regarding what constitutes an actionable injury following a data breach. Courts at all levels will continue to struggle with how to interpret and apply *Spokeo,* especially given the discrepancy in the types of data stolen in recent cases. The continuing divergence among circuits and growing risk of forum shopping eventually may compel the Supreme Court to address the issue.

Return to Table of Contents

[6] 663 F. App'x 384, 386 (6th Cir. 2016).

[7] See also, *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 968 (7th Cir. 2016) (holding that a breach involving credit card information alone crated an actionable injury); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 690 (7th Cir. 2015) (same).

[8] 870 F.3d 763, 766 (8th Cir. 2017).

[9] 848 F.3d 262, 274–75 (4th Cir.), *cert. denied sub nom. Beck v. Shulkin*, 137 S. Ct. 2307 (2017).

Massachusetts Launches Online Data Breach Reporting Portal

The state of Massachusetts announced it would debut an accessible online method of reporting data breaches for organizations with consumers in the state, offering a time-saving, streamlined reporting process to those affected by breaches.

On February 1, 2018, Massachusetts Attorney General Maura Healey announced the launch of an online portal for organizations to report data breaches that impact Massachusetts residents.[10] Before the launch of the online portal, companies were required to mail written notice of a data breach to the attorney general's office. Although the online portal will make it easier for companies to provide notice to the attorney general's office, organizations will still need to provide separate notice to any residents affected by a data breach in accordance with the state law.

Massachusetts Data Breach Notification Law

Under Massachusetts law, if an organization knows or has reason to believe that a data breach has exposed the personal information of Massachusetts residents, the organization must notify the attorney general's office, the Office of Consumer Affairs and Business Regulation (OCABR), and any affected Massachusetts residents. The notice to the attorney general's office and OCABR must include the following information:

- a detailed description of the nature and circumstances of the data breach;
- the number of Massachusetts residents affected as of the notice date;
- the steps that have been or will be taken in response to the incident; and
- information regarding law enforcement engagement in any investigation of the incident.

The notice to affected residents must include the following information:

- the resident's right to obtain a police report;
- how the resident can request a security freeze, including the information that the resident must provide to obtain such a freeze; and
- any fees to be paid to the consumer reporting agencies.

[10] The portal can be accessed here.

The Online Data Breach Reporting Portal

The online data breach reporting portal provides helpful guidance to organizations impacted by a data breach by structuring the queries to ensure that a reporting organization supplies all required information. In most cases, it suggests possible appropriate answers, which may be useful for organizations that do not have personnel dedicated to data privacy matters and may be less familiar with the data breach notification process. For example, in asking whether the affected organization has taken any actions in response to the breach, the portal provides a list of potential remediating actions (*e.g.*, consumer notice, employee training, deleted information, credit monitoring or directing the consumer to a dedicated call center). Use of the portal is not required, though organizations are still permitted to provide notification to the attorney general's office by letter.

Key Takeaways

If a company experiences a data breach affecting Massachusetts residents, the new online reporting tool may reduce the time and effort required to notify the attorney general's office as required by Massachusetts law. However, the company will still need to provide separate notice to OCABR and any affected Massachusetts residents. Although the most significant expense associated with Massachusetts' data breach notification requirements typically arises from providing notice to affected residents — not to the attorney general's office — the online portal is a helpful step towards simplifying the notification process.

Return to Table of Contents

New York State Issues Guidance for Virtual Currency Businesses

On February 7, 2018, the New York State Department of Financial Services (DFS) issued guidance concerning the policies that virtual currency business entities must have in place to prevent fraud and market manipulation.

Guidance on Preventing Virtual Currency Fraud

The DFS guidance applies to all licensed virtual currency business entities or entities chartered as limited purpose trust companies under the New York Banking Law (together referred to as VC entities),[11] and urges VC entities to adopt written policies that evaluate risk areas related to fraud, attempted fraud and similar wrongdoing, including market manipulation. The guidance emphasizes that such manipulation includes "many, varied types of wrongful activity," such as misuse of an exchange service to affect the price of virtual currency and trading on insider information with respect to a particular currency, and notes that these risks can come from employees and/or customers of the VC entities. As a result, DFS states that any VC entity must adopt a policy that:

- identifies and assesses the full range of risks;
- provides effective procedures and controls to protect against those risks;
- allocates responsibility for monitoring risks; and
- provides for period evaluation and revision.

In the event wrongdoing is discovered, the guidance requires the VC entity to file a report with DFS describing the events and provide updates on any developments, including steps taken by the VC entity to mitigate the effects of any wrongdoing and to prevent its recurrence. DFS expects the update with respect to mitigation and prevention efforts to be made within 48 hours of the initial incident report. The guidance also requires that VC entities maintain records of each incident for inspection by DFS.

Key Takeaways

The DFS guidance signals a continued effort by New York state to regulate the virtual currency industry. Companies to which the guidance applies should ensure that their risk monitoring and incident response plans are designed to enable them to comply with the DFS requirements, including timely incident reporting and record-keeping.

Return to Table of Contents

[11] A copy of the guidance can be found here.

Second Circuit Upholds Right to Privacy of Health Data Regardless of Whether Records are 'Stigmatizing'

On February 9, 2018, a three-judge panel of the Court of Appeals for the Second Circuit held that three correction officers at an upstate New York jail had a constitutional right to a privacy claim against their employer who viewed their medical records without permission, regardless of whether such records contained health information that might be viewed as stigmatizing.[12]

Background

Three correction officers at a jail in upstate New York's Rensselear County brought a suit against the jail after discovering that their health records had been accessed without their permission. A nurse working for Samaritan Hospital, which provides medical care at the jail, taped her login information for the hospital's confidential record system to the inside of her desk at the jail, which permitted jail personnel to access the hospital's record system. An investigation by Samaritan Hospital determined that the login information was used to access medical records of multiple non-inmate patients, including the plaintiffs. In March 2013, the hospital alerted patients whose records had been accessed without their permission.

The plaintiffs filed a complaint in the United States District Court for the Northern District of New York on September 20, 2013, alleging violations of their right to privacy in health information implied by the Due Process Clause of the 14th Amendment and violations of the Computer Fraud and Abuse Act (the CFAA), and alleging that the records were accessed as part of a campaign by the jail to police excessive use of sick leave. On September 24, 2014, the district court dismissed the CFAA claims for failure to state a claim, finding that the plaintiffs failed to plead economic damages. After more than a year of discovery, the district court granted summary judgment to the defendants on the 14th Amendment claims, finding that the plaintiffs did not have a constitutionally protected interest in medical privacy because the medical conditions described in their records were "insufficiently stigmatizing."

The Court's Decision

The Second Circuit affirmed the district court's determination with respect to the CFAA claims and vacated the district court's decision regarding the 14th Amendment claims, finding that people with non-stigmatizing medical conditions have a right to privacy in their medical records "even if their interest in privacy might be less."

The Second Circuit criticized the district court's emphasis on the extent to which the medical conditions contained in the improperly accessed health records were stigmatizing or serious, arguing that such an emphasis set a dangerous threshold test, stating, "If the right to privacy were to depend exclusively on the seriousness of the condition one seeks to keep private, medical records would not truly be protected from arbitrary government intrusion. It would be as if the First Amendment allowed a particular person to speak only if they could show they have something worth saying, or if the Fourth Amendment required individuals to obtain warrants to prevent the government from searching their effects."

The lower court relied on the Second Circuit's decision in another case, *Matson v. Board of Education of City School District of New York*,[13] which dealt with a school that had publicly disclosed the fibromyalgia of its music teacher in connection with a report on her alleged abuse of the school's sick leave policy. There, the Second Circuit found that the teacher's privacy rights had not been violated, after weighing her relatively weak privacy interest (she had already disclosed her medical condition and it was not as serious or stigmatizing as other conditions) against the school's interest in issuing the report to eradicate fraud and misconduct.

The panel distinguished *Matson*, explaining that the privacy concerns in *Matson* were weaker since the teacher had already disclosed her medical condition to the school. Furthermore, the court emphasized that the "shocks the conscience" test, which is applied when evaluating executive action that does not involve penological interests, must always balance the individual's interest in privacy against the government's actions. "Even the weakest privacy interests cannot be overridden by totally arbitrary or outright malicious government action," the court stated. The court clarified that, "[w]e have never held, in *Matson* or elsewhere, that only medical records documenting conditions of sufficient gravity and stigma may qualify for constitutional privacy protection."

[12] A copy of the decision can be found here.

[13] A copy of the decision can be found here.

The case was remanded back to the district court for further proceedings consistent with the Second Circuit's analysis and with instructions to consider whether the government workers named as defendants were entitled to qualified immunity (a determination the lower court did not consider, since it had found that the defendants did not have claims under the 14th Amendment).

Key Takeaways

The Second Circuit's decision clarifies that while the strength of a privacy interest is relevant to the due process inquiry, the stigmatizing or serious nature of a medical condition is not a dispositive factor in balancing an individual's right to privacy against the government's interest.

Return to Table of Contents

SEC Issues Interpretive Guidance on Cybersecurity Disclosures

On February 21, 2018, the U.S. Securities and Exchange Commission (SEC) issued an interpretive release providing guidance for public companies relating to disclosures of cybersecurity risks and incidents.

Although the guidance is unlikely to impact annual reports being filed in the near term, companies may wish to consider the new guidance in connection with preparing their proxy statements for upcoming annual meetings and other SEC filings. In addition, the guidance addresses cybersecurity considerations in connection with company disclosure controls and procedures and insider trading policies. See our February 23, 2018, client alert for a brief summary of the key takeaways from the new guidance.

Return to Table of Contents

Contacts in the Cybersecurity and Privacy Group

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5381
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Lisa Gilford
Partner / Los Angeles
213.687.5130
lisa.gilford@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

Amy Park
Partner / Palo Alto
650.470.4511
amy.park@skadden.com

Ivan Schlager
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Jen Spaziano
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

Donald L. Vieira
Partner / Washington, D.C.
202.371.7124
donald.vieira@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

William Ridgway
Counsel / Chicago
312.407.0449
william.ridgway@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000