Bloomberg BNA

Privacy and Security Law Report®



**Cybersecurity Liability**

There was no shortage of activity in the cybersecurity and data protection arena in 2015, whether in the courts, among regulators or even internationally—and in 2016, the only constant companies can count on is change, including more scrutiny, the authors write.

# Cybersecurity Liability Risks in 2016

BY NATASHA G. KOHNE, MICHELLE A. REED AND DAVID S. TURETSKY

*Natasha G. Kohne is partner at Akin Gump in Abu Dhabi. She is co-leader of the firm's cybersecurity, privacy and data protection practice, and has spearheaded Akin Gump's international data protection and cybersecurity efforts.*

*Michelle A. Reed is partner at Akin Gump in Dallas where she is co-leader of the firm's cybersecurity, privacy and data protection practice and represents public companies and their officers and directors in privacy litigation.*

*David S. Turetsky is partner at Akin Gump in Washington. He is the co-leader of the firm's cybersecurity, privacy and data protection practice.*

The year 2015 was a landmark for cybersecurity and data protection. Unprecedented European Union data protection decisions, first-time U.S. regulatory enforcement actions and record-setting data breaches highlight some of the major developments and events in these areas. As data breaches continue to dominate the headlines, 2016 will likely present continued class action and regulatory activity for companies nationwide and internationally. According to the PriceWaterhouseCoopers (PwC) 2015 U.S. State of Cybercrime Survey, 76 percent of U.S. executives and security experts are more concerned about cybersecurity threats this year than in the previous 12 months, up from 59 percent the year before, and a record 79 percent detected a security incident in the past 12 months. Companies now identify cybersecurity as their number one concern and judges and regulators will be expecting companies to assess these risks and take reasonable precautions. With breaches becoming even more prevalent, and base-level cybersecurity standards becoming more abundant and ever-evolving, liability risks will continue to increase in 2016.

 ISSN 1538-3423

## Class Action and Other Litigation Risk

Class action liability to companies is broadening, with companies involved in major data breaches facing class actions by individual consumers, merchant banks, credit card companies and others. While the legal requirement of standing/injury-in-fact continues to present a major hurdle to individual consumer class actions, plaintiffs' counsel scored a major win in 2015 that will likely have ripple effects throughout 2016. In *Remijas v. Neiman Marcus Group*, the U.S. Court of Appeals for the Seventh Circuit reversed the district court, ruling that Neiman Marcus (NM) customers whose credit card information was compromised had standing to bring a class action suit against the retailer. (14 PVLR 1351, 7/27/15) With dozens of lawsuits being filed within days of a major data breach, most major data breach class actions are now being transferred to the multi-district litigation panel in federal court. All of these issues signal that the risk of getting cybersecurity wrong will likely cost companies millions (and potentially hundreds of millions) in losses.

Individual consumers are no longer companies' biggest threats. The major card brands—e.g., Visa, MasterCard, Discover, American Express—are also shifting costs of remediation to the companies with the perceived lack of adequate information security controls. As Target Corp.'srecent settlement with the major credit card brands ($39 million with MasterCard and its merchant banks, $67 million with Visa and its merchant banks—compared to only $10 million to consumers) demonstrates, companies face real financial risk in the wake of a data breach.

**Companies should anticipate increased regulation and enforcement in the area of cybersecurity. There are a host of sectoral regulators that are revving up their activities.**

For retailers, this risk potentially became greater in the fall of 2015. Previously, across payment networks, liability for card-present fraudulent transactions was generally the responsibility of card issuers. As of October 2015, however, certain U.S. payment networks independently implemented fraud liability shifts whereby liability for some fraudulent transactions shifted to the acquirer/merchant if they do not use ''smart chip'' Europay MasterCard Visa (EMV) technology and applications to process payment transactions.

Class action liability also continues to be a threat in the health-care industry. Although health-care professionals are often more sensitized to security concerns partially due to the Health Insurance Portability and Accountability Act Security Rule, health care remains one of the most vulnerable industries, whether due to the high value of health data to criminals as compared to certain other types of data, or the difficulty of keeping up during a period of rapid regulatory and business changes throughout the sector, such as expanded use of electronic medical records or increased hospital consolidation. While most class actions to date have focused on the entity that caused the breach (e.g., if a third-party business associate suffered the breach, plaintiffs sued the business associate rather than the underlying health-care provider), the solvency of the third-party business associate also appears to have affected the likelihood of the underlying health-care provider being sued. Indeed, 2016 will almost certainly be a difficult litigation terrain for companies across many industries.

## Regulatory Risk

Companies should anticipate increased regulation and enforcement in the area of cybersecurity. There are a host of sectoral regulators responsible for parts of the energy, transportation, financial services, communications and health-care industries, among others, that are revving up their activities. But agencies with some of the widest jurisdiction are among the most active. The Third Circuit's decision in the Federal Trade Commission's (FTC) suit against Wyndham Worldwide Corp. for a series of three data breaches—acknowledging the FTC's jurisdiction to attack lax data security practices using its enforcement authority over unfair and deceptive trade practices—will likely embolden the FTC in its role as *de facto* chief cybersecurity regulator.[1]Fortunately for defendants, such authority may not go unchecked, as evidenced by the dismissal of the FTC's action against LabMD Inc.[2]

The Securities and Exchange Commission (SEC) appears similarly emboldened in the area of cybersecurity, as 2015 was the SEC's most active year to date in setting out expectations regarding cybersecurity. The SEC Office of Compliance Inspections and Examinations (OCIE) issued multiple risk alerts and announced a new audit, and the Investment Management Division issued additional guidance. To make sure everyone was listening, the SEC announced an enforcement action against RT Jones, an investment adviser, pursuant to Sections 203(e) and 203(k) of the Investment Advisers Act of 1940 under Rule 30 of Regulation S-P for its ''failure to adopt policies reasonably designed to protect customer records and information'' (14 PVLR 1749, 9/28/15). Although there was no evidence that any client suffered financial harm, the investment adviser settled for $75,000.

For multinational companies, international data protection compliance also presents a unique regulatory risk. In late 2015, the European Court of Justice issued a landmark decision in *Schrems v. Data Protection Authority*, which invalidated the Safe Harbor that allowed for transfer of data between Europe and the U.S. (14 PVLR 1825, 10/12/15). Multinational companies faced a chaotic regulatory environment, with the U.S. Department of Commerce saying it would still enforce the Safe Harbor, and some European Data Protection Authorities saying that they would prosecute companies transferring data from Europe to the U.S. relying on the now-invalidated Safe Harbor, particularly after Jan. 31, 2016. European Commissioner for Justice, Consumers and Gender Equality Vera Jourova has since announced that the EU has ''agreed in principle'' with the U.S. on

[1] *FTC v. Wyndham Worldwide Corp.*, 3d Cir., No. 14-3514, 8/24/15 (14 PVLR 1592, 9/7/15).

[2] *FTC v. LabMD* (Administrative law judge decision, currently under appeal to Commission) (14 PVLR 2109, 11/23/15).

  PVLR ISSN 1538-3423

a new trans-Atlantic data transfer agreement but no such agreement has formally materialized (14 PVLR 2168, 12/7/15).

**As data breaches dominate the headlines, directors report that cyber risk is one of their greatest concerns.**

Similarly, on Dec. 15, 2015, EU politicians and officials reached a political agreement on a new EU-wide legal framework to govern data sharing and collection and related consumer privacy rights (14 PVLR 2289, 12/21/15). It is called the General Data Protection Regulation (Regulation), and it will have a significant impact on how businesses collect, store, transfer and use data once it becomes effective. Preparation will require a significant effort. Among other requirements, the Regulation will require companies to notify regulators of any data breach that creates significant risk for the data subjects involved within 72 hours of discovery of the breach. The potential penalties for violations will increase substantially. Companies should remain vigilant in their international data protection compliance to avoid liability abroad.

## Director Liability

As data breaches dominate the headlines, directors report that cyber risk is one of their greatest concerns. Nearly 90 percent of chief executives worry that cyber threats could impact growth prospects, up from nearly 70 percent the previous year.[3] Directors continue to be faced with derivative lawsuits following major data breaches, but the risk of personal liability in these suits appears to be slim. In assessing whether directors have met their duty of due care, the court will ''look for evidence of whether a board has acted in a deliberate and knowledgeable way, identifying and exploring alternatives.''[4] In the most notable case to date, the derivative lawsuit against Wyndham Worldwide's board of directors was dismissed.[5] The court held that the directors were not grossly negligent in conducting the investigation, noting key metrics for directors: Wyndham's board had discussed the cyberattacks at 14 meetings during the relevant time frame, and the company's general counsel gave a presentation regarding the data breaches or data security at each meeting. The court also noted that the board's audit committee discussed these issues during at least 16 meetings over the same time period. Noting that the company had retained third-party technology firms to investigate each breach and recommend enhancements to Wyndham's systems, the court reasoned that the board had conducted a reasonable investigation.

## Conclusion

There was no shortage of activity in the cybersecurity and data protection arena in 2015, whether in the courts, among regulators or even internationally. In 2016, the only constant companies can count on is change, including more scrutiny. With data breaches on the rise, liability risk—from class action lawsuits to industry regulators—will follow. Companies need to keep up with the threats, their risks and the law, including expanding views of their obligations. They must continue to be vigilant both before and after data breaches to limit long-term harm.

[3] PricewaterhouseCooper's 18th Annual Global CEO Survey 2015.

[4] *Palkon v. Holmes* No. 2:14-CV-01234 (D.N.J. Oct. 20, 2014) (13 PVLR 1866, 10/27/14).

[5] *Id.*