Cybersecurity and Privacy Enforcement:  
A Roundup of 2014 Cases  
Francis J. Burke, Jr. and Steven M. Millendorf, CIPP/US

Hardly a day goes by without another front-page headline regarding a cybersecurity incident that compromised a business’ customer’s data or their own intellectual property. Besides the reputational harm (which can hurt businesses even more than the financial impacts of a data security breach), who holds companies to task for their lack of security and privacy protections? This whitepaper explores recent litigation by individuals, as well as by Federal and State regulators to keep businesses on their toes when it comes to cybersecurity.

Class Action

Class action lawsuits against businesses that suffer a data breach took an interesting turn in 2014. Historically, various courts dismissed such class action lawsuits for failure to allege a concrete harm. Since the U.S. Supreme Court case in Clapper v. Amnesty International, courts hold that plaintiffs must show a “certainly impending” harm in order to establish standing. Although Clapper was a challenge to the Foreign Intelligence Surveillance Act (FISA), district courts throughout the country have used Clapper to justify the dismissal of privacy-related class action lawsuits when the plaintiffs only show an abstract concept of injury or harm.

However, two 2014 Ninth Circuit decisions cast doubt over the reach of Clapper to deny plaintiffs standing in privacy breach class action lawsuits. In 2011, the Sony Playstation Network (PSN) suffered a data breach that exposed personal identifiable information for millions of Sony’s customers. Sony took PSN offline but did not notify customers of the breach until approximately two weeks later. Similarly, in 2013, hackers attacked Adobe Systems and obtained personal identifiable information about Adobe’s customers and Adobe delayed to notify its customers. The Sony and Adobe courts distinguished Clapper and found that although the U.S. Supreme Court used the words “certainly impending” in Clapper to articulate the requirements for Article III standing instead of the words “credible threat of harm” that is “both real and immediate, not conjectural or hypothetical” used by the Ninth Circuit precedent in Krottner v. Starbucks, Clapper did not overrule Krottner and merely reiterated the established rule that a plaintiff must sufficiently allege an “injury in fact” to establish Article III standing. Although the Ninth Circuit acknowledged that it denied standing on a number of occasions when the plaintiff’s allegations were insufficient to show an “injury-in-fact,” the Sony and Adobe courts still found the plaintiffs had plausibly alleged a credible threat of harm based on the disclosure of their personal information following the attack. The Adobe and Sony courts both found that neither Krottner nor Clapper require plaintiffs allege that an unauthorized third party actually access

---

5 Krottner v. Starbucks, 628 F.3d 1139, 1143 (9th Cir. 2010).
the plaintiff’s personal information. The Adobe court implied that, by the U.S. Supreme Court’s own statement in *Clapper* stating its standing inquiry was especially rigorous when it “certainly impending” standard should be limited to standing inquiries that involve claims that a branch of the government’s actions violate the U.S. Constitution.

In December 2014, Target was dealt a double blow against their motions to dismiss class action lawsuits brought by financial institutions and Target’s customers as a result of a data breach. Target suffered a data breach over the 2013 Christmas holiday shopping period that involved approximately 110 Million customers’ personal information including customers’ names, email addresses, and credit and debit card numbers, expiration dates, and encrypted security codes. Target delayed to acknowledge the existence and full scope of the breach, and a security blog and the Wall Street Journal first broke the news of the breach to the public instead of Target.

Target’s first blow in court was dealt on December 2, 2014 when Target’s 12(b)(6) motion to dismiss a class action lawsuit by five bank lenders on behalf of lenders nationwide was denied by the Minnesota District Court. The court held that the plaintiffs had adequately pled the elements of negligence, negligence per se, and violations of Minnesota’s Plastic Card Security Act to deny Target’s motion. The court specifically found that the plaintiff’s had pled that Target’s actions and inactions had caused the alleged foreseeable harm when it disabled certain security features, failed to heed warning signs as the hackers’ attack began, and that Target’s conduct both caused and exacerbated the harm that the plaintiffs suffered. The court also found the plaintiffs plausibly alleged that Target was solely able to and solely responsible to safeguard its and the plaintiffs’ customer data.

Second, on December 18, 2014, the same court denied Target’s 12(b)(6) motion to dismiss Target’s consumer’s class action lawsuit when it found that the plaintiffs adequately pled certain specific injuries. The court contrasted previous cases that granted defendant’s motions for dismissal for lack of standing when it found that the plaintiffs adequately pled specific injuries including unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees. The court criticized Target’s contentions that these injuries were insufficient because the plaintiffs failed to allege that these expenses were unreimbursed or if banks closed their accounts as setting too high a standard for the plaintiffs to meet at this early stage of the litigation.

The Target case is far from over, and Target may still prevail – the court left open the possibility of later dispositive motions (such as summary judgment) if discovery should fail to show the plaintiff’s allegations of harm. Target also moved that the court should dismiss the claims under the state laws of Delaware, Maine, Rhode Island, Wyoming, and the District of Columbia for lack of Article III standing because none of the named plaintiffs reside in those states. The *Target* court deferred the decision on

---

12 *Id.* at *22.
13 *Id.* at *10.
14 *Id.*
15 *Id.*
16 *Id.*
17 *Id.*
18 *Id.*
19 *Id.* at *8.*
this matter until the class certification stage and suggested that Target could renew its arguments regarding standing if the court later certifies the class and the certified class contains no members from these states.\textsuperscript{20} Furthermore, the plaintiffs will still need to show that the case meets the requirements of FRCP Rule 23(b)(3) and that common issues predominate over the individual issues of the class in order for the court to certify the class.\textsuperscript{21}

Although some courts were initially reluctant to find plaintiffs sufficiently pled “certainly impending” harm sufficient for Article III standing after \textit{Clapper}, \textit{Sony} and \textit{Adobe} suggest that plaintiffs need not plead the type of improper information use the Target customer’s alleged and some courts may be willing to find Article III standing as long as the class action plaintiffs can plead actual disclosure of their personal information.\textsuperscript{22} For example, in contrast to \textit{Sony}, \textit{Adobe}, and \textit{Target}, the District Court for the Northern District of Illinois held class action plaintiffs lacked standing against P.F. Chang’s restaurants for a data breach that released credit and debit card information when they merely alleged that P.F. Chang’s failed to comply with reasonable data security standards without any showing of actual disclosure or harm as a result of the breach, such as unreimbursed charges on their credit or debit cards (although the plaintiffs did allege that they had been notified of specific attempted fraudulent activity on their credit card by their bank).\textsuperscript{23} The \textit{P.F. Chang’s} court found the remote speculation of future harm in the increased risk of identity theft insufficient to satisfy an injury in fact required for standing.\textsuperscript{24} Thus, while \textit{Target} may indeed be the “easy” case where plaintiffs alleged actual harm, the recent class action cases against Sony Pictures Entertainment will again test the courts’ willingness to find standing in light of a data breach that (at least as currently known) only involved public disclosure of individual’s personal information.

\textbf{Federal Trade Commission (FTC) Enforcement Actions}

Even when class action litigation fails to hold a business accountable for cybersecurity and privacy, since 2006 the Federal Trade Commission (FTC) has held businesses responsible for their privacy and security promises to consumers under its power to investigate unfair and deceptive trade practices granted in Section 5 of the Federal Trade Commission Act.\textsuperscript{25} 2014 saw new investigations into security promises by consumer electronic vendors as well as challenges to the FTC’s authority to regulate data security practices under its Section 5 authority to prevent and investigate unfair and deceptive practices.

Thus far, the lower courts and a special commission have upheld the FTC’s authority to hold businesses responsible for security and privacy practices under Section 5(a).\textsuperscript{26} In \textit{FTC v. Wyndham Worldwide Corp.}, hackers gained unauthorized access to consumers’ personal information from Wyndham’s computer systems on multiple occasions.\textsuperscript{27} The FTC alleged that after Wyndham had discovered the first two attacks, it unreasonably and unnecessarily failed to take appropriate steps to prevent further unauthorized exposure of customers’ data and these failures caused, and was likely to

\begin{itemize}
\item \textsuperscript{20} \textit{Id.}
\item \textsuperscript{21} Fed. R. Civ. P. 23(b)(3).
\item \textsuperscript{22} \textit{Sony}, 996 F. Supp. 2d. at 962; \textit{See Adobe}, 2014 U.S. Dist. LEXIS 124126 at *27; \textit{Target}, 2014 U.S. Dist. LEXIS 175768, at *7.
\item \textsuperscript{24} \textit{Id.} at *2.
\item \textsuperscript{26} \textit{See FTC v. Wyndham Worldwide Corp.}, 10 F. Supp. 3d 602 (D. N.J. 2014); \textit{See Order Denying Respondent LabMD’s Motion to Dismiss, In the Matter of LabMD.}, 2014 FTC LEXIS 2, F.T.C Docket No. 9357 (January 16, 2014).
\item \textsuperscript{27} \textit{Wyndham}, 10 F. Supp. 3d at 608.
\end{itemize}
cause, substantial consumer injury (including financial injury). Wyndham challenged the FTC’s authority to assert unfair and deceptive practice claims in the data-security context. Wyndham relied on the U.S. Supreme Court holding in *FDA v. Brown & Williamson Tobacco Corp.*, to claim that Congress did not give the FTC authority to regulate data security through the FTC’s Section 5 general authority to regulate unfair or deceptive trade practices just like the U.S. Supreme Court found that the FDA did not grant the FDA authority to regulate tobacco products through its general authority to regulate drugs. The court rejected Wyndham’s motion to dismiss, stating that unlike *Brown & Tobacco*, the court could find no congressional intent to carve out data security from the FTC’s Section 5 authority to prevent unfair or deceptive trade practices, and did not find Congress’ enactment of specific data security laws, such as FCRA, GLBA, and COPPA incompatible with or to contradict this authority.

In *In the Matter of LabMD*, LabMD, a medical diagnostics company, again challenged the FTC’s Section 5 authority to regulate data security breaches as unfair trade practices. In 2013, the FTC filed an administrative complaint against LabMD that alleged it failed to reasonably protect the security of 10,000 consumers’ personal data, including medical information, and this failure to protect consumers’ information constituted unfair practices in violation of Section 5 of the FTC Act. LabMD argued that the Health Insurance Portability and Accountability Act (HIPAA) regulated it as a covered entity and therefore the FTC lacks authority to regulate its data security practices. A panel of four commissioners unanimously denied LabMD’s motion to dismiss, finding the FTC’s authority to regulate data security practices consistent with the FTC Act and its legislative history, other statutes, and extensive case law. The panel found Congress intended to delegate broad authority to the FTC to determine the definition of unfair practices. Consistent with the district court’s decision in *Wyndham*, the panel also rejected LabMD’s reliance on *Brown & Williamson Tobacco* that Congress intended to repeal the FTC’s authority to enforce data security promises when it enacted more specific data security statutes.

However, LabMD did win on its motion to compel testimony from the FTC. LabMD argued that the FTC held companies to security standards that did not adequately notify companies of the standards that the FTC uses. The FTC’s Chief Administrative Law Judge ruled in May 2014 that the trial court can compel the FTC to disclose the data security standards used to determine if a company uses reasonable security standards, and specifically that the FTC must provide deposition testimony that describes what security standards, if any, it has published and that it intends to rely on at trial. This may provide companies a first opportunity to obtain more specificity from the FTC about the data security standards it uses in data breach enforcement actions.

---

28 Id. at 609.
29 Id. at 607.
31 *Wyndham*, 10 F. Supp. 3d at 607.
32 Id. at 613.
33 See *LabMD*, 2014 FTC LEXIS 2 (January 16, 2014).
34 Id. at *4.
35 Id. at *3.
36 Id. at *7-17.
37 Id. at *9.
38 Id. at *29.
40 Id. at 6.
While the FTC was battling challenges to its authority from Wyndham and LabMD, it still had an opportunity to hold companies responsible for security and privacy claims that turn out to be false. For example, on December 31, 2014, the FTC settled complaints with Snapchat over false claims regarding the disappearing nature of messages sent through its service, its collection of geolocation and contact information, and its failure to secure certain features of its service.41

In one novel Section 5 enforcement action, the FTC held a company responsible for security claims it made for an “Internet of Things” consumer product for the first time in history.42 In its September 2013 Complaint, the FTC alleged that TRENDnet engaged in unfair or deceptive practices when it manufactured and sold home Internet Protocol (IP) Cameras that it marketed as “secure” through package labeling, in product descriptions on TRENDnet’s website, and in other advertisements but that failed to actually provide reasonable security.43 The FTC alleged that TRENDnet’s security failures arose from the transmission and storage of user login credentials in unencrypted form, a failure to actively monitor security vulnerability reports from the public, and a failure to use reasonable and appropriate security practices in the design and testing of the software that it provided to consumers.44 The FTC specifically alleged that a hacker had reviewed the software TRENDnet provided consumers, discovered a flaw in a setting that allowed the hacker to view all live feeds from consumers’ IP cameras, and later posted information about the breach along with links to approximately 700 consumer IP cameras.45 The FTC alleged that the compromised live feeds showed the private areas of consumers’ homes, and permitted the unauthorized viewing of infants, children, and adults, and that news articles had shown photos taken from the compromised live feeds.46

In February 2014, the FTC entered a final Decision and Consent Order (Consent Order) against TRENDnet.47 The Consent Order prohibits misrepresentations by TRENDnet about the security of any Internet-accessible device sold by TRENDnet or how any of its products and services maintain and protect individually identifiable information transmitted through such a product.48 TRENDnet must also establish, implement and afterwards maintain a comprehensive security program appropriate with its size and complexity, the nature of its activities, and the sensitivity of the device and information.49 As is common with many of the FTC’s Consent Orders, TRENDnet must also submit to an initial and ongoing monitoring of its compliance every two years for the next twenty years.50 TRENDnet must also notify the affected consumers about the details of the security flaw and the information that may have been revealed.51

**Federal Communications Commission (FCC) Enforcement Actions**

While the courts have thus far affirmed the FTC’s authority to regulate the security practices of most companies, Section 5 of the FTC Act explicitly withholds the FTC’s authority to prevent unfair

43 Id. at 3.
44 Id. at 4.
45 Id. at 5.
46 Id.
48 Id.
49 Id.
50 Id. at 5.
51 Id. at 6.
and deceptive practices of common carriers, such as telecommunication companies. The FCC regulates these entities and for the first time held telecommunication carriers liable for failing to adequately protect consumers’ privacy.

In September 2014, the FCC settled a complaint with Verizon Wireless that alleged that since 2006 Verizon accessed new customers’ customer proprietary network information (CPNI) for marketing purposes before they notified consumers of their privacy rights, including how to opt out of marketing. In an FCC press release, the FCC claimed FCC regulations require that telecommunications companies notify the FCC within five (5) days when the opt-in or opt-out process is not working properly, but Verizon waited 126 days after they became aware of the issue. The Consent Decree requires Verizon pay $7.4 Million to the U.S. Treasury (at the time, the largest payment in FCC history for a privacy-related settlement), requires Verizon to include opt-out notices on every bill instead of just the first bill, and requires Verizon to monitor and test its billing systems and opt-out notice process for compliance.

The FCC also initiated its first data security case and largest privacy action in history: the FCC stated on October 24, 2014 that it plans to fine two Lifeline telephone carriers, TerraCom, Inc. and YourTel America, Inc., $10 Million for violations of several privacy laws. The FCC alleged that the companies stored customers’ Social Security Numbers, names, addresses, driver’s licenses, and other sensitive information it collected in connection with the Lifeline program on unprotected servers that could be accessed by anybody over the Internet. The allegations include claims that the companies: (i) failed to properly protect consumers’ personal information (PI); (ii) failed to use reasonable security practices to protect consumers’ PI; (iii) engaged in deceptive and misleading practices when the companies falsely represented to consumers that they used appropriate technologies to secure the consumers’ PI; and (iv) engaged in unjust and unreasonable practices when the companies failed to fully inform consumers that third-parties had compromised their PI.

Notably, two FCC commissioners dissented in the decision. One commissioner stated that he does not believe that the Communications Act contains any pre-existing duty on carriers to use reasonable security practices to protect consumers’ PI or to notify consumers of a breach of PI. The second commissioner dissented on the grounds that he did not believe that the FCC had any authority to act under the Communications Act (specifically that Section 222 does not contemplate protection of the type of consumer information disclosed here), and even if it did, the FCC should not hold TerraCom and YourTel responsible in this case because it has not provided fair notice that there could be liability for such conduct.

---

55 Consent Decree at 7, 16, In the Matter of Verizon, FCC DA-14-1251.
59 Id. at 25-30.
60 Id. at 25.
61 Id. at 27.
Shareholder Derivative Suits

In addition to class action lawsuits by those impacted by a data breach and regulatory investigations, shareholders have also tried to hold board members liable for cybersecurity incidents through shareholder derivative lawsuits, and 2014 was no exception. Target shareholders filed at least four shareholder derivative lawsuits in early 2014 against Target’s directors and officers in the District Court of Minnesota. While all of the cases allege a breach of fiduciary duty and waste of corporate assets, Davis additionally alleges gross mismanagement and abuse of control. The complaints all similarly allege that the defendants were aware of the importance of the security of personal customer information to Target’s customers, and the risks of a data security breach. Each of the complaints allege that Target, through its officers and directors, failed to implement reasonable and appropriate security measures to protect customers’ personal and financial information, “failed to take reasonable steps to have [Target] notify customers that their information had been compromised,” and although aware of the high risk of a data breach, “failed to implement any internal controls… designed to detect or prevent [a data breach].”

The shareholder complaints make a point to emphasize that not only did the board fail to take steps to detect and prevent the breach, but the board also aggravated the damage when it failed to provide prompt and adequate notification of the breach to affected customers and when Target released multiple misleading public statements that conveyed a false sense of security to customers.

The complaints further allege that these failures severely damaged the company, and note that the company is under investigation by the United States Secret Service and the Department of Justice as well as the growing multitude of class action lawsuits against the company (with one complaint counting at least sixty-seven such class action lawsuits and thirty additional investigations by various state Attorney Generals). All of the complaints claim that the class action lawsuits expose the company to hundreds of millions of dollars in liability.

---


Each of the Target shareholder cases are still pending, and the defendants have yet to file responsive pleadings in these cases or otherwise raise defenses. The defendants will likely raise the defense that they properly supervised Target’s security practices under the business judgment rule and raise the defense that each case should be dismissed for an inadequate pre-suit demand even though each complaint asserted the futility of such a demand.

Companies can sometimes successfully use the business judgment rule defense when they act quickly to investigate cybersecurity incidents and inform themselves of cybersecurity issues that face their companies. Shareholders that brought an action against Wyndham Worldwide Corporation in 2014 had their case quickly dismissed by a New Jersey District Court judge when the judge found the business judgment rule protected Wyndhams’ officers’ and directors’ actions. Shareholders brought an action against Wyndham’s directors and officers for alleged violations of law, breach of fiduciary duties, and waste of corporate assets that arose from three separate data breaches between April 2008 and January 2010. Similar to the Target complaints, shareholders alleged that board’s failure to implement appropriate internal security controls to detect and protect against data breaches severely damaged the company. Wyndham’s shareholders additionally alleged that the failure to timely disclose the breaches in the Wyndham’s financial statements aggravated the damages.

Unlike the Target shareholders, on at least two separate occasions Wyndham shareholders demanded the board bring a lawsuit against the company based on the breaches and, in each instance, the board formed a committee that decided that the shareholder’s complaints were not well grounded and insufficient to bring an action against the company. The District Court of New Jersey disagreed with the plaintiffs’ arguments that the board inadequately investigated the complaint when it decided to reject the shareholders’ demands, and specifically pointed to quarterly general updates the board received about data security, the fact that the board discussed the security breaches in at least sixteen committee meetings to try to understand what happened and to determine appropriate remedies, and the fact that the board members had previously developed an understanding of the breaches through the FTC investigation. Furthermore, the court noted that the board did not summarily dismiss the shareholder’s demands, and instead the board specifically met to discuss them and voted unanimously not to pursue it.

The Target and Wyndham shareholder derivative cases show that although plaintiffs may face difficulty to overcome strong presumption that the business judgment rule shields the board’s actions, directors and officers of companies that experience cybersecurity incidents will likely continue to face claims for liability for the company’s cybersecurity policies and procedures, as well as their cybersecurity incident responses. Directors and officers will likely continue to escape liability if they promptly investigate such incidents and fully inform themselves about the incident, become fully informed about changing cybersecurity risks to their specific company and industry, and reasonably plan for cybersecurity incidents and there responses to such incidents.

73 Id. at 3 ¶¶ 5.
**State Attorney Generals**

State Attorney Generals also play a critical role to investigate the impacts of security breaches that involve the personal information of their states’ residents. In 2014, state Attorney Generals from across the country investigated security breaches at retailers such as Target, Neiman Marcus, Michaels, and Home Depot, as well as at banking institutions such as J.P. Morgan Chase.

In one notable new 2014 case, the California Attorney General filed a complaint against insurance company Kaiser Foundation Health Plan for an unreasonable delay in Kaiser’s notification to individuals after a hard drive that contained the personal information (including Social Security Numbers, dates of birth, addresses, etc.) of Kaiser employees was sold at a thrift store. This marks the first time that the California Attorney General brought an action arising out of a delayed security breach notification. California’s breach notification law requires that a person or business that conducts business in California notify individuals affected by a breach in the most expedient time possible and without unreasonable delay. Although the statute does not explicitly define the terms “most expedient time possible” or “without unreasonable delay,” the California Office of Privacy Protection recommends that such notice be within 10 business days of the determination that consumer personal information was, or reasonably believed to have been, acquired by an unauthorized third person (with acceptable delays for law enforcement investigation). The California State Attorney General alleged that Kaiser engaged in unfair competition (as defined by California Business and Professions Code § 17200) when it (a) failed to timely disclose the security breach to the affected individuals in violation of California’s breach notification law, and (b) made unencrypted social security numbers on the hard drive available to the public in violation of California Civil Code § 1798.85. In particular, the complaint alleges that Kaiser could have notified at least some individuals affected by the breach as early as December 2011, but waited until mid-March 2012 before it notified California residents of the breach. Kaiser entered into a stipulated judgment in February 2014 that requires it to notify individuals affected by future breaches on a rolling basis and to implement additional information security training programs. Kaiser was also fined $30,000 and required to pay an additional $120,000 in attorney’s fees for the cost and prosecution of the matter.

**SEC Perspective and Duty to Warn Shareholders.**

Starting at least as early as 2011, the Securities and Exchange Commission (SEC) began to analyze if its existing regulations directed towards the integrity of market systems and the disclosure of material information adequately protected market participants against cybersecurity risks. In a speech on June 10, 2014, Commissioner Luis Aguilar noted the severe impact that cyberattacks may have on 

---

80 Cal. Civ. Code § 1798.82.
82 Id. at 2 ¶ 5.
84 Id. at 3 ¶ E.
capital markets and on public companies and their investors, and advocated that companies expand
directors’ roles to prepare for and respond to cybersecurity incidents.86

In October 2011, the SEC’s Division of Corporation Finance issued guidance that indicated that the SEC considers the requirements to “disclose timely, comprehensive, and accurate information about risks that a reasonable investor would consider important to an investment decision” includes the disclosure of cybersecurity risks and cybersecurity incidents.87 The guidance suggests that public companies should “evaluate its security risks” and “take into account all available information” to determine if the risk of a cybersecurity incident must be disclosed.88 Every public company should consider both the internal and external impacts to customers from a cybersecurity incident and review the adequacy of its preventative measures in the context of its particular risks, known threats, and standard industry practices.89

The SEC’s guidance suggests that the disclosure of cybersecurity risks may need to meet the general risk factor disclosure requirements of Regulation S-K Item 503(c) and describe the nature of the cybersecurity risks and how each cybersecurity risk may affect the company.90 These disclosures may include: (a) the company’s business or operations exposed to the cybersecurity risk and the potential costs and consequences of a cybersecurity incident; (b) a description of any outsourced functions with material cybersecurity risks, if any; (c) a description of any material cybersecurity incidents (either individually or in the aggregate) and the costs and consequences of those incidents; (d) risks associated with prolonged undetected cybersecurity incidents; and (e) a description of the company’s cybersecurity or other relevant insurance.91 Furthermore, the SEC suggested that public companies may need to disclose known previous or threatened incidents to properly put these risks in context.92

Despite the relative focus by the SEC on public companies’ cybersecurity disclosure requirements, it is unlikely that the SEC will bring any formal actions against companies in the near future. However, it seems inevitable that the SEC will hold companies who ignore these disclosure guidelines responsible sometime in the future and CFOs should begin to understand their company’s cybersecurity risks and responses and begin to address these cybersecurity issues in the company’s ongoing reporting and disclosure requirements.

Conclusions

2014 marked a milestone in cybersecurity – by September 2014, there were 1,922 confirmed cybersecurity incidents that compromised almost 1 Billion records worldwide, up 81% from 2013 (which was already up 493% from the 92 million records in 2012).93 Many of the incidents widely reported in 2014 resulted in the compromise of one 1 Million or more records, and it should come as no

---

88 Id.
89 Id.
90 Id.
91 Id.
92 Id.
surprise that as the number and severity of these incidents go up, so does the attempts to hold companies responsible.94

The year 2015 should be no different – we expect to see some closure to some of the remaining actions brought in 2014, including the multiple actions and investigations brought against Sony Pictures Entertainment as a result of the breach which involved intellectual property in the form of its upcoming movies (costing the company millions in lost revenue), but also emails, social security numbers, home addresses, financial and health records of celebrities and its employees (the total price tag, including the damage done to its systems, loss of productivity, and settlement of the lawsuits likely to run into the hundreds of millions of dollars)95. Nobody should expect hackers to take a holiday during 2015 – it is more likely that 2015 will bring additional breaches of larger magnitude. While the courts and regulatory bodies will be as busy as ever as they try to fit these cybersecurity breaches into aging bodies of law, companies should continually review their security practices and be prepared to defend themselves on multiple fronts in the event of a cybersecurity incident.

---

1 Francis J. Burke, Jr. is a partner and litigation lawyer with Foley & Lardner LLP where his practice emphasizes complex civil and criminal litigation and trials, including individual, multiparty and class action claims and complex civil and criminal parallel proceedings. He also focuses on white collar criminal defense, antitrust and securities enforcement and other governmental enforcement actions, and state and federal false claims matters. Mr. Burke’s practice spans the financial services, technology, health care, life sciences, manufacturing, computer, software, Internet, defense contractor, real estate, hospitality, aerospace and defense, accounting and energy industries. Mr. Burke has been recognized in The Best Lawyers in America© since 2007 for Commercial Litigation and White Collar Criminal Defense, in the 2007-2011 and 2013-2014 California Super Lawyers® lists for Securities Litigation, and in Chambers USA: America’s Leading Business Lawyers from 2007 through 2012 for General Commercial Litigation. He has been Peer Review Rated as AV® Preeminent™, the highest performance rating in Martindale-Hubbell’s peer review rating system. Mr. Burke frequently speaks on diverse topics, including the False Claims Act, health care, pharmaceutical and government contractor whistleblowers, securities litigation, eDiscovery, retention of electronic documents, electronic and digital evidence, the use of technology pretrial and in trial, trade secrets, corporate internal investigations, securities liability of officers and directors, computer crimes, developing corporate compliance programs, representing high-tech companies, international litigation, partnering between inside and outside counsel, using experts, and basic trial and deposition skills. He has written and spoken extensively on eDiscovery and has worked with litigation support databases for most of his career, most recently with large e-mail populations. Recently, he co-authored the article, “FTAIA Analysis: 7th Circ. vs. 2nd Circ.,” Law360 (August 5, 2014).

ii Steven M Millendorf is an associate and intellectual property lawyer with Foley & Lardner LLP. He has experience drafting, reviewing and revising technology agreements, including protections for privacy and data security. Mr. Millendorf regularly tracks changes to state breach notification laws and revises Foley’s nationally published state data breach notification database. Prior to his legal career, Mr. Millendorf worked extensively as an security ASIC design engineer at various companies. His memberships include the Intellectual Property Law Section of the American Bar Association, where he is on the Online Data, Transactions, and Security Committee, and the Science & Technology Law Section of the American Bar Association, where he is on the E-Privacy Law, Homeland Security, Information Security, Privacy and Computer Crime Committees. He is also a Certified Information Privacy Professional (CIPP/US) by the International Association of Privacy Professionals (IAPP).

94 Id.