ZELLE HOFMANN

ZELLE HOFMANN VOELBEL & MASON LLP

2011 — The Year of The Breach

Consumers, companies, insurers, and legislators stake out positions after rash of data breaches

By Karl S. Vasiloff and Christine T. Phan
Published in *Insurance Law360*

In the first seven months of 2011, a number of companies and institutions have reported large-scale data breaches. The causes of the breaches range from misplacement of data by employees to malicious hacking by organized hacker groups.

Direct and indirect victims of these attacks include many well-known names. In February, Nasdaq reported that its confidential data sharing service had been compromised. In March, the security firm RSA revealed that data related to its popular SecurID token technology had been stolen in a cyberattack. In April, Epsilon, the world's largest email marketing provider, reported that data on customers of 50 retailers, including US Bank, JP Morgan Chase, Capital One, Citi, the Home Shopping Network, Best Buy, Target, and Verizon, was exposed to an unauthorized entry into Epsilon's email system. Also in April, the Office of the Texas Comptroller realized that it had inadvertently disclosed the Social Security numbers of 3.5 million people. In May, Citigroup reported that hackers had obtained information on over 360,000 credit card accounts. In June, a programming bug that left cloud service provider Dropbox's 25 million user accounts accessible with any password sparked a class action lawsuit over potential personal information exposure. In July, the Pentagon revealed that it had suffered massive losses of sensitive data after a cyber attack by a foreign government. Perhaps drawing the most media attention, Sony fell victim to what has been called the largest data breach ever, affecting nearly 77 million users of Sony's Playstation and Qriocity services by an organized group of hackers. These serial breaches have led some commentators to appropriately nickname 2011 "The Year of the Breach."

Consumer Class Actions

With 77 million users affected, Sony may incur record costs relating to its data breaches. Immediately following the breaches, Sony predicted that breach remediation measures alone would cost the company at least $171 million. Included in this amount are insurance and free identity theft protection offered by Sony to affected customers, including an insurance policy providing up to $1 million in coverage for identity theft. In addition, Sony hired a private security firm to find the source of the breaches. However, Sony's $171 million estimate did not include any costs related to consumer lawsuits which, perhaps inevitably, followed closely on the heels of the breaches being reported. Several putative class actions have been filed against Sony with complaints alleging negligence, invasion of privacy, misappropriation of confidential financial information, breach of implied contract, and breach of express contract. Disgruntled consumers have filed a total of 55 breach-related suits against Sony in the United States alone. One

Canadian suit filed on behalf of Canadian Playstation users alleges damages in excess of $1 billion. It appears that such damages claims will not be uncommon in consumer data breach lawsuits. A suit alleging $3.5 billion in damages was recently filed against the Office of the Texas Comptroller in connection with the data breach it experienced earlier this year. The suit comes on top of the $1.2 million the Comptroller has already spent notifying affected individuals.

Consumer data breach lawsuits are not a new phenomenon but until recently, plaintiffs involved in data breach actions have enjoyed limited success because of their inability to demonstrate that a data breach caused them a legally cognizable injury. In particular, many courts have not accepted plaintiffs' claims for damages for the future risk of identify theft, leaving data breach plaintiffs largely unable to move past the motion to dismiss stage. *See, e.g.*, *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629 (7th Cir. 2007).

Recently, however, data breach plaintiffs achieved what could be a game-changing victory. In *Claridge v. RockYou*, *Inc.*, No. C 09-6032 (N.D. Cal. Apr. 11, 2011), plaintiff Claridge is advancing a novel damages theory. RockYou is a developer of applications for use with networking sites like Facebook that allow users to share photos and play games with other users. After RockYou's servers were breached in 2009, Claridge alleged that RockYou failed to secure its users' personally identifiable information (PII). Claridge took the position that since users essentially "pay" for RockYou's products by providing PII, PII is valuable property that the users exchanged for products, services, and RockYou's promise to use commercially reasonable methods to protect the PII. Claridge claimed that when RockYou's database was breached, he and other users lost the value of their PII. The Court found that Claridge had alleged an injury in fact sufficient to support Article III standing. The Court's decision was rendered with skepticism, however:

> Not only is there a paucity of controlling authority regarding the legal sufficiency of plaintiff's damages theory, but the court also takes note that the context in which plaintiff's theory arises – i.e. the unauthorized disclosure of personal information via the Internet – is itself relatively new, and therefore more likely to raise issues of law not yet settled in the courts. For that reason, and although the court has doubts about plaintiff's ultimate ability to prove his damages theory in this case, the court finds plaintiff's allegations of harm sufficient at this stage to allege a generalized injury in fact.

The Court then noted that, if through discovery it is revealed that no basis for recovery exists for plaintiff, the court will then dismiss the suit for lack of standing. *RockYou* may seem like a small success for plaintiffs, but advancing a consumer data breach lawsuit into discovery actually represents a significant victory for aggrieved consumers, as many companies may be unwilling to shoulder the significant costs associated with discovery in a lawsuit of this nature.

New Laws, New Recourse, New Costs, New Lawsuits

In addition to legal fees, companies that have experienced data breaches could potentially face fines from the Federal Trade Commission and state governments for violation of privacy laws. Sony, for example, is also now under investigation by the attorneys general of several states for violation of the various states' privacy laws. Indeed, a number of existing laws pertain to the protection and sharing of personal information, including the Federal Trade Commission Act (FTC Act), Gramm-Leach-Bliley Act, the Fair and Accurate Credit Transaction Act, and the Health Insurance Portability and Accountability Act (HIPAA). In addition, 46 states have laws which require businesses to notify consumers when PII has been lost or stolen. A study by the Ponemon Institute found that the existence of breach notification laws substantially increases the costs of handling a data breach in the United States as compared to the UK, Germany, Australia, and France.

Though numerous privacy laws are already in place, legislators have proposed several new bills in response to the back to back data breaches. The addition of new laws regulating the storing and sharing of personal information will undoubtedly increase the costs associated with future breaches. The White House recently proposed a comprehensive cybersecurity legislation which calls for an overarching national data breach notification law that would preempt existing state notification laws. The proposed law would be enforced under the FTC Act as an unfair or deceptive act in commerce and would allow state attorneys general to impose civil penalties of up to $1,000 a day per affected individual up to a maximum of $1,000,000 per violation unless the conduct is willful or intentional, in which case the civil penalty would not be capped.

Moreover, companies which have not suffered breaches at the hands of hackers have also come under fire from consumers who are becoming more cognizant of how customer PII is handled on a daily basis. In what the *Wall Street Journal* termed "a new breed of consumer class-action litigation," over 100 large retailers, including Tiffany & Co, Coach, Nordstrom, Macy's, and Wal-Mart, are now the subject of lawsuits concerning the retailers' collection of customer zip codes during in-store purchases in alleged violation of state privacy laws. After the California Supreme Court ruled that zip codes are PII which retailers are prohibited from requesting under California's Song-Beverly Credit Card Act of 1971 in February, a flurry of law suits followed. Allegedly, retailers had been using customer zip codes to deduce customers' full addresses to sell to other companies. The putative classes are seeking civil penalties up to $1000 for each time each customer was asked to provide his zip code over the past year.

Cyberinsurance

With the potentially extraordinary costs of remedying a breach and breach-related litigation, affected companies are turning to their insurers. Insurers are responding that claims arising out data breaches are not covered under traditional insurance coverage. For example, Hartford Fire Insurance (Hartford) filed declaratory judgment actions seeking a determination that Hartford has no duty to defend Children's Place Retail Stores and Crate & Barrel in connection with the zip code lawsuits. Hartford's denial is

based on language which excludes coverage for damages "arising out of the violation of a person's right of privacy created by any state or federal act." Indeed, the passage of new privacy laws with higher protections for individual rights of privacy may have the effect of making it harder for insureds to claim coverage for data breaches in light of such exclusions. Sony also tendered the class action lawsuit complaints and investigative inquiries to its insurer, Zurich, for defense and indemnification. Zurich also disclaimed coverage for the consumer lawsuits and on July 22, sought a declaratory judgment that it had no duty to indemnify Sony because the claims in the class action lawsuits did not allege bodily injury, property damage, personal injury or advertising injury. In the past, insureds have found only spotty success claiming that data breaches fall under the traditional categories of property damage or personal and advertising injury.

Even before Zurich's denial of coverage, the spate of data breaches had brought renewed attention to cyberinsurance – a specialized insurance product intended to protect companies against hacker attacks and data breaches. Though insurance carriers began marketing cyberinsurance as an alternative form of coverage in the late 1990's, in terms of popularity, cyberinsurance languished for years, with only one-third of American companies reported to be holding such policies in 2009. Thus far, companies found the cost of cyberinsurance prohibitive and the application process complicated and expensive for both the insurer and applicant.

Interestingly, Sony reportedly has a cyberinsurance policy, but appears to have sought defense and indemnification from its commercial general liability carrier (Zurich), perhaps because its cyberinsurance does not offer coverage for the types of costs Sony has incurred due to the breach or simply because its cyberinsurance does not offer an adequate amount of coverage. Indeed, another obstacle to cyberinsurance gaining traction in the past was the fact that it was difficult for carriers to quantify the exact scope of an applicant's cyber risk due to the sheer scale and scalability of the internet.

However, the proliferation of both breaches and the resulting consumer class actions has allowed insurers and insureds to gain a better understanding of the type and scope of risks and associated costs involved in a sizeable data breach. Equipped with the knowledge of what to expect in the aftermath of a data breach, insurers can better assess their potential exposures when underwriting a policy for new cyberinsurance customers. With the recent wave of well-publicized and large-scale breaches, companies are seizing the opportunity to renew a marketing push for cyberinsurance and security products. Beazley, for example, markets that it is on the cutting edge of cyberinsurance, focusing on healthcare, retail, hospitality and higher education markets. Beazley's advertised coverage includes noncompliance fines and expanded coverage for voluntary notification in cases of breaches which do not trigger a legal duty to notify. Cyberinsurers are also tailoring their products to the specific needs of certain industries. Hiscox USA advertises that it offers specialized HIPAA coverage for the "unique exposures faced by the healthcare industry."

The insurers' marketing efforts are well-timed. Even though cyberbreaches are not a new phenomenon, public disclosure of such breaches and the resulting public pushback

are forcing companies to begin to manage and mitigate risks of cyberbreaches with new measures, including tougher security on the front end and cyberinsurance on the back end. Reuters reports that demand is now soaring for cyberinsurance. Demand will likely increase from here as reports of cyberattacks gain more momentum. In a white paper released on August 3, the security firm McAfee noted that "every company in every conceivable industry with significant size and valuable intellectual property and trade secrets has been compromised (or will be shortly), with the great majority of the victims rarely discovering the intrusion or its impact. In fact, . . .the entire set of Fortune Global 2000 firms [can be divided] into two categories: those that *know they've been compromised* and those that *don't know yet*." The white paper revealed a 5-year long cyberattack on 72 entities by one specific, unidentified actor (code-named "Operation Shady RAT") which targeted the governments of the United States, Canada, and South Korea, the United Nations, and commercial entities spanning a wide range of industries, including construction, energy, real estate, and sports.

The relentless breaches that have helped this year earn its nickname show no signs of slowing down. Certainly, in this year alone, significant change has come to the financial, legal, political, and insurance realms due to the data breaches in the form of increased consumer awareness, new business practices, landscape-changing lawsuits, sweeping proposed legislation, and an emerging insurance product — and it's only August.

*****

Karl Vasiloff (kvasiloff@zelle.com) is a partner at Zelle Hofmann Voelbel & Mason LLP in the firm's Boston, Massachusetts office. Christine Phan (cphan@zelle.com) is an associate at the firm's Boston office. Zelle Hofmann is a national law firm representing clients in their most challenging insurance-related disputes, antitrust claims and other complex litigation. For additional information about Zelle Hofmann, please visit www.zelle.com.