Contemporary Legal Notes

Washington Legal Foundation
Advocate for freedom and justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302

DATA BREACHES:
LITIGATION STRATEGIES AND COMPLIANCE MANAGEMENT

By
Arti Sangar
Diaz Reus, LLP

Washington Legal Foundation
CONTEMPORARY LEGAL NOTE Series

Number 74
June 2013

TABLE OF CONTENTS

ABOUT WLF'S LEGAL STUDIES DIVISION

The Washington Legal Foundation (WLF) established its Legal Studies Division to address cutting-edge legal issues by producing and distributing substantive, credible publications targeted at educating policy makers, the media, and other key legal policy outlets.

Washington is full of policy centers of one stripe or another. But WLF's Legal Studies Division has deliberately adopted a unique approach that sets it apart from other organizations.

First, the Division deals almost exclusively with legal policy questions as they relate to the principles of free enterprise, legal and judicial restraint, and America's economic and national security.

Second, its publications focus on a highly select legal policy-making audience. Legal Studies aggressively markets its publications to federal and state judges and their clerks; members of the United States Congress and their legal staffs; government attorneys; business leaders and corporate general counsel; law school professors and students; influential legal journalists; and major print and media commentators.

Third, Legal Studies possesses the flexibility and credibility to involve talented individuals from all walks of life – from law students and professors to sitting federal judges and senior partners in established law firms.

The key to WLF's Legal Studies publications is the timely production of a variety of intelligible but challenging commentaries with a distinctly common-sense viewpoint rarely reflected in academic law reviews or specialized legal trade journals. The publication formats include the provocative COUNSEL'S ADVISORY, topical LEGAL OPINION LETTERS, concise LEGAL BACKGROUNDERS on emerging issues, in-depth WORKING PAPERS, useful and practical CONTEMPORARY LEGAL NOTES, interactive CONVERSATIONS WITH, insightful ON THE MERITS, and law review-length MONOGRAPHS.

WLF's LEGAL OPINION LETTERS and LEGAL BACKGROUNDERS appear on the LEXIS/NEXIS® online information service under the filename "WLF" or by visiting the Washington Legal Foundation's website at www.wlf.org. All WLF publications are also available to Members of Congress and their staffs through the Library of Congress' SCORPIO system.

To receive information about previous WLF publications, contact Glenn Lammi, Chief Counsel, Legal Studies Division, Washington Legal Foundation, 2009 Massachusetts Avenue, NW, Washington, D.C. 20036, (202) 588-0302.

ABOUT THE AUTHOR

Arti Sangar is a partner with the law firm Diaz Reus, LLP in Dubai, United Arab Emirates. She specializes in commercial dispute-resolution and arbitration, transactional matters involving private equity investments, corporate-restructuring, mergers and acquisitions, major real estate development projects, commercial dispute management, and employment issues.

Ms. Sangar co-authors *Emirates Business Law Blog* (www.emiratesbusinesslaw.com), which is focused on business and law in the Middle East.

DATA BREACHES:
LITIGATION STRATEGIES
AND COMPLIANCE MANAGEMENT

by
Arti Sangar
Diaz Reus, LLP

Data loss and security breach incidents have become an all-too-common event. Seemingly, each day, large amounts of private information are being unlawfully accessed or disclosed. "Unfortunately, companies and institutions of all sizes are vulnerable to serious peer-to-peer related breaches, placing consumers' sensitive information at risk," warned then-Federal Trade Commission (FTC) Chairman Jon Leibowitz[1].

Major data breaches over the past year involving companies like LinkedIn Corporation,[2] Yahoo,[3] and Zappos[4] triggered multi-million dollar lawsuits alleging failure to safeguard private information. Bank accounts, medical records, and contact information are among the data which has been breached, exposing these major companies to reputational damage beyond the obvious commercial and financial ramifications. As a result, companies should

---

[1] *See* Widespread Data Breaches Uncovered by FTC Probe, Federal Trade Commission Alert, Feb. 22, 2010 available at http://www.ftc.gov/opa/2010/02/p2palert.shtm.

[2] *See* Nicole Perlroth, *Lax Security at LinkedIn Is Laid Bare,* N.Y. TIMES, June 10, 2012, available at http://www.nytimes.com.

[3] *See Yahoo Breach Extends Beyond Yahoo to Gmail, Hotmail, AOL Users*, N.Y. TIMES, July 12, 2012, available at http://www.nytimes.com.

[4] *See Zappos Suffers Security Breach; Customers Emails And Passwords Affected*, HUFFINGTON POST, Jan. 16, 2012, available at http://www.huffingtonpost.com/2012/01/16/zappos-suffers-security-b_n_1208194.html.

anticipate such a data breach and should stay abreast of industry best practices for data security.

Claims arising from data breaches have included, amongst others, actions for negligence, breach of fiduciary duty, invasion of privacy, and actions under consumer protection and data breach notification laws. Data breach litigation routinely takes the form of a class-action lawsuit brought on behalf of consumers whose personal information has potentially been compromised.

Although reporting of data breaches has significantly increased, many lawsuits related to these incidents have not been successful. The problems plaintiffs face include selecting the right cause of action and proving damages. Some plaintiffs have attempted to bring claims in situations where their information has not been used and where they are merely claiming the possibility that there will be damages in the future. A number of courts have looked at these issues as questions of standing. For example, some courts have ruled that plaintiffs in cases of data breaches did not have standing to bring claims for future damages, on the ground that an alleged increase in risk of future injury is not an actual or imminent injury in fact.

This LEGAL NOTE will survey how U.S. courts have treated data breach cases, assess why plaintiffs have had such difficulty finding success in this arena, and identify the relevant data protection laws in the U.S. It also presents strategies that companies can employ to mitigate the risks of data security breaches, including practical advice on establishing compliance

procedures and formulating privacy policies.

I. STANDING IN DATA BREACH LAWSUITS

Every plaintiff must demonstrate standing to bring a data breach lawsuit. However, standing is just one of the initial hurdles for any would-be plaintiff. In most data breach lawsuits, plaintiffs allege that defendants were negligent in allowing the data to be disclosed or misused. In order to bring a lawsuit for negligence, plaintiffs need to establish that (a) the defendant had a duty to protect data; (b) there has been a failure to protect data; and (c) the plaintiff has incurred damages directly and proximately caused by that failure.

A. Duty to Protect Data

A company's duty to provide security may come from several different sources – but the net result is a general obligation to provide security for all private data and information systems. In other words, information security is no longer just good business practice – it is a legal obligation. A company is particularly liable where there is a fiduciary relationship as between a bank and its client, a doctor and her patient, or a teacher and his student.

Two cases, both involving a duty to provide security generally, illustrate this point. In *Wolfe v. MBNA America Bank*,[5] a federal court held that where injury resulting from negligent issuance of a credit card is foreseeable and preventable, the defendant has a duty to verify the authenticity and accuracy of a credit account application before issuing a credit card. In *Bell v. Michigan*

[5] *See Wolfe v. MBNA America Bank*, 485 F. Supp. 2d 874, 882 (W.D. Tenn. 2007).

Council,[6] the court held that where harm was foreseeable, and the potential severity of the risk was high, the defendant was liable for failure to provide appropriate security to address the potential harm.

Repeated failures to protect customer data have also led the FTC to recently file a data breach lawsuit against the hotel operator, Wyndham Worldwide.[7] In this case, the FTC alleged that Wyndham's poor security led to hundreds of thousands of consumers' credit card information to be exported to an Internet domain address registered in Russia.

On the flip side, in *Guin v. Brazos Education*,[8] the court held that where the defendant conducted a proper risk assessment and a particular harm was not reasonably foreseeable, the defendant would not be liable for failure to defend against it. Similarly, the court in *Giordano v. Wachovia Securities*[9] held that a customer lacked standing to bring a claim as to future identity theft. The court cited the plaintiff's failure to allege that she suffered an injury-in-fact that was either actual or imminent and not a mere possibility.

Because the case law continues to evolve, questions still remain as to information security practices and parameters that businesses in different industries should meet.

---

[6] *See Bell v. Michigan Council*, 2005 Mich. App. Lexis 353 (Feb. 15, 2005).

[7] *See Fedral Trade Commission v. Wyndham Worldwide Corporation; Wyndham Hotel Group, LLC; Wyndham Hotels & Resorts, LLC; and Wyndham Hotel Management, Inc.* (FTC File No. 1023142, Case No. 2:12-cv-01365-SPL), First Amended Complaint for Injunctive and other Equitable Relief at Page 15; available at http://www.ftc.gov/os/caselist/1023142/120809wyndhamcmpt.pdf.

[8] *See Guin v. Brazos Higher Education Service Corporation, Inc.*, 2006 WL 288483 (D. Minn. 2006).

[9] *See Giordano v. Wachovia Securities, LLC*, 2006 WL 2177036 (D.N.J. 2006).

B. Failure to Take Reasonable Care

Courts and regulators are becoming increasingly sensitive to whether a business has reasonable security to protect the personal information they hold from misuse and loss. *PATCO Construction Inc. vs. Ocean Bank*[10] raised questions about reasonable security and liability. In 2010, PATCO sued Ocean Bank, alleging that the bank's security system was not commercially reasonable and that it had not consented to security procedures, after thousands of dollars were stolen from its accounts. The First Circuit ruled in favor of PATCO, finding that the bank's data security was commercially unreasonable under the Uniform Commercial Code.[11]

Similarly, in *Experi-Metal Inc. (EMI) vs. Comerica Bank*,[12] EMI sued Comercia Bank, seeking to hold the bank liable for approximately $560,000 in stolen funds that were not recovered. In the ruling, the court found that Comerica Bank should have identified and disallowed the fraudulent transactions, based on EMI's history, which had been limited to transactions with a select group of domestic entities. The court also noted that Comerica's

---

[10] *See Patco Construction Company, Inc. v. People's United Bank Case*, No. 11-2031 (C.A. 1, Jul. 3, 2012).

[11] Article 4A of the Uniform Commercial Code ("UCC"), as codified under Maine Law at Me. Rev. Stat. Ann. tit. 11, § 4-1101 *et seq.*

[12] *See Experi-Metal, Inc., v. Comerica Bank* (Docket Number: 2:2009cv14890) (E.D. Mich. June 13, 2011), Bench opinion available at http://www.gpo.gov/fdsys/pkg/USCOURTS-mied-2_09-cv-14890/pdf/USCOURTS-mied-2_09-cv-14890-3.pdf.

knowledge of phishing[13] attempts aimed at its clients should have caused the bank to be more cautious.

The rulings in these cases suggest that courts are expanding the duty of corporations and are beginning to flesh out the scope of "reasonable security" and "good faith" in the context of data protection.

C. Injury

In the past, courts have inconsistently applied the Article III[14] standing requirement in data security breach litigation. Some courts have even held that the mere threat of identity theft is sufficient to confer standing.[15] Whereas, on the other hand, other courts have held that the mere danger of future harm does not satisfy the injury requirement.[16] A recent U.S. Supreme Court ruling, however has provided a resolution to these conflicts. On February 26, 2013, the Court clarified in *Clapper v. Amnesty International*[17] that the

---

[13] "Phishing" is described as the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information. *See* http://www.webopedia.com/term/p/phishing.html.

[14] Article III of the U.S. Constitution grants federal courts the power to adjudicate certain "cases" or "controversies." This constitutional case-or-controversy clause provides the foundation for the doctrine of standing, a threshold inquiry plaintiffs must satisfy before a federal court may exercise subject-matter jurisdiction over a claim. Among other requirements, a plaintiff must show that he has suffered an "injury in fact" that is actual or imminent and not just conjectural or hypothetical.

[15] See *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) (holding, on issue of first impression, that class-action plaintiffs had standing where they alleged threat of identity theft).

[16] *See Reilly v. Ceridian Corp.*, 664 F.3d 38, 43 (3d Cir. 2011), (cert. denied, 132 S. Ct. 2395 (2012) (affirming dismissal of case for lack of standing where risk of future harm was alleged.

[17] *Clapper v. Amnesty International USA*, No. 11-1025.

mere threat of future harm does not satisfy Article III's injury requirement. In *Clapper*, the plaintiffs had sought to challenge the constitutionality of § 1881a of the Foreign Intelligence Surveillance Act, which authorizes the federal government to conduct surveillance on certain communications between parties located in the United States and parties outside the United States for the purpose of acquiring intelligence information.

The Second Circuit ruled that the plaintiffs had established standing because they had demonstrated reasonable fear that their communications could be monitored and had taken costly measures to avoid being monitored. The Supreme Court overturned this decision, holding that the plaintiffs did not have legal standing to sue because they could not demonstrate that their future injuries were "certainly impending."

The Supreme Court's decision in *Clapper* has broad implications for data security breach litigation. Corporations facing data breach litigation can rely on *Clapper* when moving to dismiss the complaint on the ground that plaintiffs lack the Article III standing. A strong argument can be made that under *Clapper*, the unpredictability of third-party criminals undermines any claim that harm is "imminent".

II. NAVIGATING U.S. DATA PRIVACY LAWS

The U.S. has yet to enact a single, comprehensive federal law regulating the collection and use of personal data. For now, parties must contend with a patchwork system of federal and state laws and regulations that overlap, dovetail, and even contradict one another. In addition, there are many

guidelines, developed by governmental agencies and industry groups, that are not legally enforceable but are considered "best practices."

Certain industries are subject to legal obligations to protect sensitive data. These obligations were broadly created through the enactment of federal privacy legislation in the financial services, health-care, government, and Internet sectors. The Gramm-Leach-Bliley Act[18] regulates the collection, use, and disclosure of consumer information and applies to financial institutions such as banks, insurance companies, securities firms, and other businesses that provide financial services and products. Also, the Health Insurance Portability and Accountability Act[19] regulates medical information. It can also apply broadly to data processors, health care providers, pharmacies, and other entities that come into contact with medical information.

In order to address data breaches outside of those areas where a specific federal law governs, the Federal Trade Commission relies upon the Federal Trade Commission Act.[20] The Act is a federal consumer protection law that prohibits unfair or deceptive acts or practices. The FTC has brought numerous enforcement actions against corporations for failing to comply with their own privacy policies and for the unauthorized disclosure of personal data. In defense of the FTC's suit against them, Wydham Worldwide is challenging the

---

[18] Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6827.

[19] 42 U.S.C. § 1301 et seq.

[20] Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (The federal statute establishing the Federal Trade Commission (FTC) and empowering it, among other duties, to prevent unfair methods of competition and unfair or deceptive acts or practices affecting interstate commerce.

Commission's authority to punish companies accused of data breaches under the "unfairness" authority contained in the FTC Act.

In addition to the federal laws, most states have enacted some form of privacy laws that regulate the collection and use of personal data.

III. PRACTICAL ADVICE AND STRATEGIES

A. Compliance

It is essential that businesses be aware of their obligations to those persons whose personal data they hold, and have in place appropriate policies and procedures to monitor and ensure compliance. A comprehensive compliance system can help companies avoid the potential minefields and reduce the potential risks associated with non-compliance, particularly in view of the growing body of law in this area and the existing obligations provided under data protection laws. Thus, a critical starting point for preventing data breaches is developing policies for handling personal information and the implementation of regular training programs. Companies with an international presence also must comply with the data protection laws of each jurisdiction where they operate.

B. Breach Notification

Companies that experience a data breach may be required to notify affected individuals. With data breach incidents on the rise, most states have enacted notification statutes that require businesses to publicly acknowledge data breaches so that affected parties can take appropriate precautions. For example, California's notification statute, the Security Breach Information

Act[21] was the first notification statute in the nation. Many states have used California's notification statute as a template for their own legislation. Although quickly informing consumers of data breaches allows them to take proper precautionary measures, it can also lead to increased litigation on behalf of customers.

C. Litigation Tactics

From a plaintiff's perspective, the best course of action is likely to initiate a class action lawsuit, if the plaintiff can demonstrate actual injury. As discussed above, however, class actions can also face a key hurdle to success in the U.S. Plaintiffs must prove the individuals affected by the breach were actually injured. Many data breach cases do not have such concrete injuries. Class actions, therefore, are not a guaranteed avenue of recovery. In other words, class actions do not give plaintiffs a free pass – plaintiffs must have the standing to bring their claims.

Although class action plaintiffs face obstacles to recovery, defendants should not expect to avoid penalties for data breaches. Defendants should make efforts to avoid protracted and expensive litigation and to consider entering into a quick and confidential settlement with plaintiffs. For example, after hackers stole customer information from TJX Companies[22] in 2007, the company quickly entered into a settlement agreement with the affected consumers. In the settlement, TJX Companies agreed to provide a certain

---

[21] *See* 24 CAL. CIV. CODE § 1798.82 (West 2007).

[22] *See In re TJX Cos. Retail Sec. Breach Litig.*, 584 F. Supp. 2d 395, 401 (D. Mass. 2008).

number of affected consumers with three years of credit monitoring and compensate affected consumers. While a class action settlement may prove expensive and burdensome to the settling defendant, it can offer many benefits. Most notably, a settlement provides the defendant with a degree of certainty regarding to its potential exposure.

IV. FUTURE CHALLENGES

As data breaches continue to rise, so too will enforcement actions and litigation. Companies are under tremendous pressure to protect data. The cost of data protection is also on the rise because of the need to comply with laws requiring more stringent security measures. The development and implementation of data protection policies and practices and the frequent monitoring of data security systems have also increased compliance costs for companies. Employee training for data security maintenance has likewise grown in importance and expense. An additional issue of concern is the difficulty of maintaining security when companies outsource data to third parties. Outsourcing can be complicated because third parties are not, in practice, bound to the same standards of privacy as the company itself.

Given the complexity and expense of responding to data breach incidents, the availability of financial protection through insurance coverage tailored to data breach losses has also become a significant and growing area of attention. A robust compliance program is the key to avoiding data breaches. It is also prudent for businesses to consult with counsel in advance of a data

breach to ensure that all available measures have been considered and, if appropriate, implemented.

