ZURICH®

# Data breaches can pose huge risks for bank directors and officers

# Data breaches can pose huge risks for bank directors and officers

News reports that the FBI recently has begun investigating data security breaches at several banks—including some large financial institutions—are stark reminders that no commercial entity can fully shield itself from cyber criminals.[1]

## Introduction

Shareholders within several companies recently victimized by data security breaches have launched lawsuits against the enterprises' boards, claiming that executive management breached its fiduciary duty by failing to ensure that the companies implemented adequate security measures. What could be a developing legal trend raises the specter that no less than their personal wealth is at stake for directors and officers who do not exercise appropriate oversight of their organizations' cyber risks. Citing a litany of alleged information technology missteps, negligence and shortsightedness, the shareholders argue that the defendants' lack of attention to data security made their organizations particularly vulnerable to data thieves.

Always hunting for new litigation opportunities, the plaintiffs' bar very well could view these lawsuits as templates for shareholder actions against other organizations targeted by cyber criminals. With studies showing that the number and cost of cyber attacks against commercial enterprises are rising—and more so in the financial institutions and banking sector than in others—directors and officers at banks today cannot afford to ignore these developments.

Executive management at banks, however, also can use this shareholder litigation to their advantage. Those lawsuits provide directors and officers some clear guidance on the level of data security protection they should be pressuring their own organizations to adopt to protect themselves against cyber criminals.

## The numbers behind the risk

Banks walk a very high tightrope with customer data, but it is a dangerous act that the market demands they perform if they are going to be competitive. Customers demand 24-hour access to their accounts through multiple channels, such as ATMs, home and work computers and their smartphones while out in public.

Greater convenience for customers, however, can also mean increased opportunities for cyber criminals.

Organizations that suffer data security breaches already face the expense of restoring their data security, reconstituting corrupted data and, as statutes in 47 other states plus the District of Columbia mandate, notifying their customers and clients that their personal information has been compromised. In addition, although they generally are not legally required to do so, these organizations typically provide credit monitoring services to their customers in an effort to maintain, or regain, their goodwill.

Overall, according to the Ponemon Institute's "2014 Cost of Data Breach Study: Global Analysis," the average cost of a corporate data breach is $3.5 million, a 15 percent increase compared to Ponemon's findings in 2013.[2]

A significant factor that is driving up those costs is the growing volume of data security incidents. That number is exploding, according to a survey conducted by PricewaterhouseCoopers in cooperation with magazines CIO and CSO.[3] In that survey,

1. D. Yadron, E. Glazer, D. Barrett. FBI Probes Possible Hacking Incident at J.P. Morgan. Aug. 28, 2014. The Wall Street Journal. online.wsj.com

2. 2014 Cost of Data Breach Study: Global Analysis. May 2014. Ponemon Institute. securityintelligence.com

3. The Global State of Information Security Survey 2014. PricewaterhouseCoopers, CIO magazine, CSO magazine. pwc.com

9,681 corporate executives from companies of all sizes in 115 countries reported that each of their organizations faced 3,791 security incidents on average over the 12 months prior to February 2013. That is more than 10 incidents every day and reflects a nearly 27 percent increase from the number reported in the year-earlier survey and a 48 percent jump from the 2012 survey results. Those events included "any adverse incident that threatens some aspect of computer security," not only successful major data breaches, the study's authors explain.

The numbers were even worse for financial institutions. Those survey respondents reported not only a 22 percent higher rate of incidents—4,628 annually on average, or nearly 13 incidents each day—but also an alarming 169 percent increase over the prior year's results.

Among the financial institution respondents, 42 percent were from North America. Some 43 percent of the respondents represented either mid-sized or small organizations, and 41 percent represented large institutions. The size of the remaining respondents was unknown.

*The PwC financial institutions survey respondents reported a 22 percent higher rate of incidents, an average of 13 incidents each day.[8]*

Financial institutions, like all organizations, could face even greater challenges in mitigating cyber risk in the near future. A U.S.-like law that would impose notification responsibilities on organizations that suffer data security breaches but also impose stiff financial penalties on those deemed lax in their efforts to safeguard data likely will be in place in the European Union by 2016.[4] But the law would reach far beyond Europe, because it would apply to all organizations operating there, not just those headquartered within its borders. Moreover, many other countries are in the process of enacting or likely will adopt comparable measures to maintain their trading status the European Union, suggests broker executive Christopher Keegan, a senior managing director at Beecher Carlson in New York, and law firm Baker Hostetler, which has studied data privacy laws around the world.[5]

## Shareholder derivative-action lawsuits

With their increased exposure to headline-grabbing cyber attacks, the banking sector is heavily exposed to reputational and brand risk, regulatory actions and monetary losses. Depending on the resulting financial hit the institution takes, any and all of that fallout could trigger derivative-action lawsuits and even securities class actions.

In a derivative-action lawsuit, shareholders sue directors and officers on behalf of the organization, typically demanding that they implement new or modified procedures or protocols designed to protect the entity from specified risks. In these types of cases, shareholders do not seek damages for themselves. But they do in securities class-action lawsuits, which typically are filed following a significant drop in share price after an organization discloses a significant problem.

That litigation risk seems to be manifesting.

In separate derivative-action lawsuits, shareholders are demanding that two companies that lost their customers' and clients' personal data to cyber criminals shoulder additional costs to harden the organizations' data security systems.[6] [7] In those cases, filed against the boards of a major retailer and a hotel/resort chain, the plaintiffs allege the companies' data security systems as well as the organizations' responses to major attacks against those systems left customer data unreasonably vulnerable.

4. EU Data Protection Directive. epic.org

5. 2014 International Compendium of Data Privacy Laws. 2014. Baker Hostetler bakerlaw.com

6. Maureen Collier, derivatively on behalf of Target Corp. vs. Gregg W. Steinhafel, et al. U.S. District Court for Minnesota. January 2014.

7. Dennis Palkon, derivatively on behalf of Wyndham Worldwide Corp. vs. Stephen P. Holmes, et al. U.S. Diestrict Court for New Jersey. May 2, 2014.

8. PricewaterhouseCoopers

The list of plaintiffs' allegations include that one or both of the companies:

- Failed to take reasonable measures to prevent a security breach by, among other things, failing to comply with the PCI Data Security Standard.
- Relied on computer servers with an operating system that was so badly out-of-date that its security software had not been updated for three years. As a result, customers' credit card information was stored unencrypted.
- Had no internal controls designed to either detect a security breach or report it in a timely manner.
- Immediately after the attack, issued false and misleading statements about the significance of the security breach. It initially denied, but later admitted, that customers' debit card PIN numbers had been stolen. It also suggested the security breach affected far fewer customers and over a shorter period that it actually did.
- Damaged its reputation by hiding the true extent of the attack in order to prevent scaring away customers, causing a drop-off of holiday-season revenue.
- Gave customers a false sense of security and further harmed them by failing to provide the timely information they needed to mitigate the risk to their personal information.
- Created more bad will and further harmed customers by bungling its offer of aid after finally alerting customers and offering credit-monitoring services. In attempting to generate favorable public relations by disclosing how it was providing these services, the company created an opening for other identity thieves to scam the company's customers. In emails, the identity thieves posed as the company and obtained the customers' payment card information.
- Understood, because of the findings of a well-known independent 2007 report on data security, the risk and likely ramifications of a massive security breach.

The shareholders are demanding that the defendants reimburse their companies for the harm the executives allegedly caused and that the companies harden their data security systems. Specifically, the plaintiffs demand that the defendants directors and officers cover their organizations' remediation costs, including the cost of notifying affected customers and clients and establishing credit-monitoring services for them, as well as the organizations' costs to investigate the breaches internally and to respond to the resulting regulatory inquiries and consumer class-action lawsuits.

In addition, the plaintiffs are asking for the disgorgement of compensation paid to the individual directors and officers and payment of plaintiffs' attorney fees.

A retailer's data security breach highlights the importance of directors and officers also ensuring that their organizations have solid vendor management controls in place. Financial institutions can help to mitigate vendor risks through a combination of contract provisions and insurance.

In addition, many federal regulatory agencies have opined on vendor risk and how banks can manage it, including the:

- Federal Reserve Board, in its December 2013 guidance, Managing Outsourcing Risk.
- Office of the Comptroller of the Currency, in its October 2013 guidance on third-party relations.
- Federal Financial Institutions Examination Council, in its October 2012 discussion on information technology service providers.
- Consumer Financial Protection Bureau, in its April 2012 bulletin.

## Securities exposure

Data breaches also increase directors' and officers' exposure to regulatory action and, potentially, securities class-action lawsuits.

*Data breaches also increase directors' and officers' exposure to regulatory action and securities class-action lawsuits.*

The derivative lawsuits filed against the retailer and hotel/resort chain are instructive, particularly their demands for reimbursement of the companies' costs to respond to various state and federal investigations. In one instance, the data breach has become the subject of a lawsuit filed by a federal regulator. While regulatory activity is trouble enough for a company, it often—as was the case here—precipitates a derivative action.

The two derivative lawsuits also spend considerable time reciting numerous privacy laws designed to protect consumer information as well as various disclosure requirements as evidence that the defendants were aware of the significant risk associated with a cyber breach.

As further evidence that the defendants were aware of that risk, both lawsuits point to the companies' financial statements. In those documents, the companies provide risk disclosures on data breaches and represented that their internal controls were sufficient to guard against them, the plaintiffs state.

The focus on disclosure is important. In October 2011, the Security and Exchange Commission's Division of Corporate Finance issued guidance stressing that registrants may be obligated to discuss cyber risks and incidents under "a number of disclosure requirements" or when necessary to ensure that other required disclosures are not misleading.[9] The sections of the financial statement in which registrants may be obligated to make those disclosures are:

- Risk Factors, if that information would be a critical factor in investors' decision making.
- Management's Discussion and Analysis of Financial Condition, and Results of Operations, if those risks and incidents were materially costly; the consequences associated with any incident are material; that information indicates an important trend; or those risks and incidents create significant uncertainty for the organization.
- Description of Business, if an incident has affected the organization's product, service, customer relations, suppliers or competitiveness.
- Legal Proceedings.
- Financial Statement Disclosures.
- Disclosure Controls and Procedures. If a cyber incident could affect the quality of those disclosures, then management has to consider whether those disclosures have been rendered ineffective.

9. Cybersecurity. CF Disclosure Guidance: Topic No. 2. Oct. 13, 2011. Division of Corporation Finance Securities and Exchange Commission. sec.gov

The derivative lawsuits' focus on financial statement disclosures about cyber risk, allegations of insufficient internal controls, as well as the allegations of a potential decrease in earnings could be fodder for a securities class-action lawsuit.

To raise a securities class-action claim, a plaintiff generally must allege that the defendant knowingly, or with reckless disregard for truthfulness, made a false statement of material fact and that the plaintiffs relied upon it, causing the plaintiffs damage. Typically, plaintiffs allege that they purchased securities based on representations in a company's financial statement and that the plaintiffs suffered damages when the company's share price dropped after revelations that those representations were misleading or false.

The derivative lawsuits appear to allege all the essential elements—except for an actual drop in share price—necessary to raise a securities class-action lawsuit.

Given the increasing frequency of data security breaches and the greater emphasis on disclosure and management of internal controls, directors and officers should expect to face securities class-action lawsuits in the wake of a breach, if it triggers a market reaction.

## Insurance protection

While directors and officers can be a driving force in their organizations' efforts to fend off data thieves, data security experts warn that cyber criminals will not be discouraged easily. In the event of a successful attack, executive management who has demonstrated strong oversight of their organization's cyber risk controls would have a strong argument that they and the entity took all reasonable steps to safeguard customer data and, therefore, should not face regulatory penalties or shareholder litigation.

Still, shareholders may sue. Even if a court eventually dismisses the case because the board had done all it could to ensure that the organization had robust data security, the cost of a defense could be significant. So besides ensuring that they are meeting their fiduciary duties relating to cyber risk, executive management should ensure they are comfortable with the amount of directors and officer's liability insurance their organizations have purchased.

## Conclusion

Cyber criminals are relentless. Studies show they will attack an organization's data security system multiple times daily in many ways from different areas of the globe in an attempt to steal customers' personal data.

In an environment in which customer data is increasingly under attack, banks must take extraordinary steps to remain competitive and compliant with numerous regulations and statutes. Managing cyber exposure must be a critical element of every organization's risk management philosophy.

Moreover, directors and officers have to do more than merely trust that their organizations will be vigilant, because shareholders demand strong board leadership on data security.

*Because it's not just if an attack is going to occur, but when.*

A1-112004073-A (10/14) 112004073

Zurich
1400 American Lane, Schaumburg, Illinois 60196-1056
800 382 2150 www.zurichna.com



ZURICH®