Four Ways For A Financial Institution To Minimize Losses Related To A Data Breach

Dec 29 2014

Posted By: Mark E. Schmidt & Brion T. Winters & Mark F. Foley & William E. Taibl

Practice Area: Banking and Commercial Finance

The explosive growth of electronic credit and debit card transactions has increased the possibility of data breaches for financial institutions. The ongoing data breach litigation by financial institutions against Target is just one example of what could be the new normal with card-swipe electronic transactions now dominating commerce: according to Javelin Strategy and Research, only about twenty-five percent (25%) of point-of-purchase sales are currently made with cash, and that percentage is expected to continue to decline in the coming years.

This surge has been beneficial to the bottom line of many financial institutions, but the spike in electronic transactions has also increased the potential for data breaches and related liability. According to the Ponemon Institute's *2014 Cost of Data Breach Study: Global Analysis*[1] the average cost of a data theft from financial services companies in 2013 was $236 per customer account. The primary reason for the increase is the loss of customers following the data breach. Financial services providers continue to be most susceptible to high rates of customer defections as a result of data breaches. (*Ponemon*, 2014)

As the volume of electronic transactions has increased, hackers and cybercriminals have become more sophisticated and successful, as evidenced by recent high-profile data breaches involving Target, Neiman Marcus, eBay, and Jimmy John's. While mega-breaches tend to grab the headlines, most data losses involve fewer than 10,000 customer records. (*Ponemon*, 2014) Nonetheless, these data losses can be costly, averaging $5.9 million per breach incident in 2013. (*Ponemon*, 2014)

What can financial institutions do to minimize their losses, when both large and small institutions can fall victim? Below are four proactive steps that may be taken by any size institution:

1. Preparation
Statistically, four factors are most important to reducing the cost of a data breach: a strong pre-incident security posture, a current incident response plan, business continuity management involvement, and leadership by a Chief Information Security Officer. Together, these can reduce the per capita cost of a data breach as much as 30%. (*Ponemon*, 2014) Good preparation should also include data security audits and breach response exercises to test preparedness.

2. Purchasing Data Breach and Other Insurance

One in three companies has insurance to protect against data breach losses (Marsh LLC, *Benchmarking Trends: Interest in Cyber Insurance Continues to Climb*, 2014)[2]. Covered risks typically include disclosure of confidential data, malicious or accidental loss of data, introduction of malicious codes or viruses, crisis management and public relations expenses, business interruption expenses, and data or system restoration. In 2013, cyber insurance policies sold to retailers, hospitals, banks, and other businesses jumped significantly. (*Marsh LLC*, 2014) Given the potentially tremendous costs associated with a data breach, cyber insurance policies are no longer a niche or specialty product, and are quickly becoming a necessity in the financial services industry and a key component of risk management for financial institutions.

In addition to policies specifically covering data breaches, it is important to consider whether an institution's losses may be covered under the terms of an existing policy. Some courts have found that traditional policies include coverage for data breach claims. In *Netscape Communications Corp. v. Federal Insurance Co.*, decided in 2009, the Ninth Circuit Court of Appeals held that personal and advertising injury coverage in a commercial general liability ("CGL") policy applied to claims alleging that the insured had violated the plaintiff's right of privacy in private online communications. In *Retail Ventures, Inc. v. National Union Fire Insurance Co.*, the Sixth Circuit Court of Appeals found that coverage may also apply under a financial institution's crime policy. In *WMS Industries, Inc. v. Federal Insurance Co.*, the Fifth Circuit Court of Appeals affirmed the district court's holding that all-risk and first-party property policies may provide coverage for data damage and business interruption arising out of data breaches. Lastly, in *Retail Systems, Inc. v. CNA Insurance Companies*, the Minnesota Court of Appeals found that an insured's loss of a computer tape containing third-party data was "property damage" and, therefore, was covered by CGL insurance.

Even if there may be a question as to whether coverage is available, notice of the breach should be given to the insurer immediately. Financial institutions should consider consulting with their insurance providers to confirm whether or not their standard policies cover data breaches and, if so, whether there are any coverage limits or exclusions. "Too often, the close scrutiny of policy coverage does not occur until after a claim is made. This makes misunderstanding and disappointment a distinct, and potentially costly, risk. Even sophisticated companies stumble. In 2011, SONY suffered a series of cyber security breaches affecting data in its online gaming systems. The SONY insurer said the company did not have a cyber insurance policy, that SONY's existing policies only covered tangible property damage, not cyber incidents, and therefore the insurer would not provide any coverage for the company's nearly $200 million loss. SONY spokespersons contested these statements, expressing their belief that at least some of the losses were covered. (Mark F. Foley, *Digital Lex: Insurance Coverage for the Cyber World (Feb. 19, 2013)*, at http://www.WTNNews.com. *See*, *Insurance Against Cyber Attacks Expected to Boom*, New York Times online, December 23, 2011)

Banks, or their counsel, should also proactively review vendor or third-party contractor agreements to confirm that the vendor or third party contractor has an obligation to indemnify the financial institution for losses related to a data breach, and that the financial institution is named as an additional insured under the vendor's or third-party contractor's insurance policy covering such breaches. Contracts that do not provide these protections should be updated.

3. Using Regulatory Tools and Guidance

In September 2014, FDIC Chairman Martin Gruenberg stated that "internet cyber threats have rapidly become the most urgent category of technological challenges facing our banks." As a result, the FDIC now defines cybersecurity as "an issue of highest importance" for itself and the Federal Financial Institutions Examination Council.

The FFIEC recently formed a Cybersecurity and Critical Infrastructure Working Group that works with the intelligence community, law enforcement and the Department of Homeland Security on cybersecurity issues. The Working Group is currently assessing the banking sector's preparedness to combat and respond to cybersecurity threats. The report will include a regulatory self-assessment to evaluate readiness and identify areas requiring additional attention.

The FDIC also created a "Cyber Challenge" online resource that features videos and a simulation exercise. As part of this effort, the FDIC also requires third-party technology service providers (TSPs) to update financial institutions on operational threats the FDIC identifies at a TSP during an examination.

The rollout of these resources, coupled with the recent guidance from the OCC and the Fed regarding the management of third party relationships (for a more in-depth discussion, please see our January 2014 *Law Update*, "Managing Third Party Relationships: New Regulatory Guidance for Banks"), demonstrates the increased scrutiny regulators are giving to these issues and why they are hot-button topics for financial institutions to tackle.

4. Filing Lawsuits Against Parties Responsible for Data Breaches
A recent example of financial institutions going on the offensive with regard to a data breach by a service provider is the lawsuit brought by several banks against Target, *In re Target Corporation Customer Data Security Breach Litigation*, Case No. 14-md-02522, which is currently pending in Minnesota federal district court. The banks are seeking class-action status for banks across the country arising out of the compromise of at least 40 million credit cards, which affected up to 110 million people whose personal information, such as email addresses and phone numbers, were stolen.

The banks seek millions of dollars of damages to recover money spent reimbursing fraudulent charges and issuing new credit and debit cards.

The court recently denied Target's motion to dismiss all of the claims, concluding that Target played a "key role" in the data breach. In denying the motion, the court held that "Plaintiffs have plausibly alleged that Target's actions and inactions – disabling certain security features and failing to heed the warning signs as the hackers' attack began – caused foreseeable harm to plaintiffs" and also concluded that "Plaintiffs have also plausibly alleged that Target's conduct both caused and exacerbated the harm they suffered." At this stage, the banks are proceeding with claims for negligence and violations of Minnesota's Plastic Security Card Act.

As illustrated by the *Target* litigation, if losses are not covered by insurance or if the institution otherwise cannot be made whole, a financial institution should consider trying to recover damages through litigation. However, the *Target* case is still being litigated, and the law is not settled as to whether third parties, such as merchants who process credit and debit cards, may be held liable to an issuing financial institution for damages arising out of the merchant's data breach.

Financial institutions would be well-served by utilizing these resources to protect against cyber attacks and should keep a close eye on upcoming regulatory guidance in this area as it is clear that the regulators are focusing on ways to protect against, and minimize the number of, data breaches and their effect on financial institutions.

von Briesen & Roper, s.c. has robust banking and data privacy and security practice groups that can handle any and all legal needs of financial institutions relating to data breaches. Whether a financial institution is developing data security policies or a data breach response plan, considering litigation, arbitration, or mediation, negotiating or reviewing third-party service agreements or auditing compliance, reviewing insurance policies, or seeking assistance on regulatory compliance and risk management, von Briesen & Roper is well equipped to meet the needs of its financial institution clients. Please contact us with any questions or needs in this emerging field of banking law.

[1] Available at http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis.
[2] Available at http://usa.marsh.com/NewsInsights/MarshRiskManagementResearch/ID/37546/Benchmarking-Trends-Interest-in-Cyber-Insurance-Continues-to-Climb.aspx.
