

Community Banks

Customer Data: Some Upcoming Developments

By Kevin Rankin, CNA Insurance

When Anna Bernanke, the wife of the Federal Reserve Chairman, recently had her wallet stolen during a Capital Hill coffee stop, consumers were again reminded that everyone is vulnerable to identity theft. According to court documents, cyber thieves started cashing checks from Mr. and Mrs. Bernanke's checking account soon after her purse was stolen, entangling the high-profile couple into a "sophisticated" ring that racked up \$2.1 million in losses and involved 10 financial institutions.¹⁾

Customer data is one of a bank's most important assets, and a much-publicized identity theft such as Mrs. Bernanke's serves to remind directors and managements once again they have a custodial responsibility to protect "any and all" private and confidential information (including that of employees) in their possession. Fortunately, many community banks have made customer data protection a top priority. According to its bi-annual technology survey released in October 2008, the Independent Community Bankers of America (ICBA), a respected trade association, ID theft was the top security threat (85%) of community banks under \$100 million in assets.²⁾ Because of their size and possible lack of resources, smaller community banks are perceived to be more vulnerable to attack. Larger banks, according to the survey, are more concerned about insider data theft. The declining economy, waves of corporate layoffs, and corporate reorganizations could leave employees disgruntled and internal controls weakened. Further, an increase in mergers and acquisitions could cause important data to be scattered amongst a variety of divisions.

There are signs regulators will re-focus on IT management and cyber protection issues in 2010. During this recession, federal regulators have been justifiably concerned with rectifying problematic construction loans, toxic investment securities, and low capital levels. However, as community banks return to profitability, regulators could begin to turn their attention to how well banks are managing their back-office technology. In a glimpse of possible things to come, the FDIC has issued 11 C&D orders since spring for inadequate IT oversight.³⁾

There is speculation by some bank consultants that in 2010 the FDIC could also start to implement the broadened guidelines it imposed for remote deposit capture, an increasingly popular method of processing checks.⁴⁾ In January 2009, the Federal Financial Institutions Examination Council (FFIEC) released stringent guidance on remote capture risks and controls. Since then, with its focus more on bank financials, the FDIC has granted an "unofficial grace period". With regulatory scrutiny returning to IT next year, now is the time to be sure proper remote capture risk management is in place.

Also in 2010, two federal court cases could clarify the extent to which third-party institutions, such as community banks, can be held liable for cyber theft. In the first case, an Indiana couple sued their bank after a data security breach sent \$26,500 from their home equity line of credit to a bank in Austria. They alleged the bank had several violations, including that its on-line security was behind industry standards and "not state-of-the-art" at the time of the theft.⁵⁾ In early August, a U.S. District judge denied the bank's motion to dismiss the case and allowed it to proceed to a jury trial next year. In the second case, a construction company in Maine alleged its community bank failed in "one of its most basic obligations, namely, to protect its customers' funds against theft."⁶⁾ Similarly, in this suit, the construction company alleged the bank's security measures were lax and it should have done more to prevent hackers from stealing \$500,000 from its accounts. Regardless of their outcomes, both

federal cases clarify the extent to which banks must go to sufficiently protect their customers' confidential information against cyber theft.

With such heightened consumer, regulatory, and judicial awareness, banks should consider allocating some of their IT spending to cyber insurance. Old-school Bankers Bland Bonds or general liability policies were designed to cover "tangible" property such as money or securities from named perils like robbery or fire, not this new generation of cyber risks. To address this computer-generated exposure, the insurance industry has developed a variety of cyber insurance products. Products vary greatly, but buyers should consider policies that:

- Respond to breaches of both on-line and off-line data, by outsiders and by rogue employees.
- Provide data coverage from the theft or loss of removable media (such as bank-owned laptops and PDAs) and paper records, from any location.
- Cover privacy injury resulting from the unauthorized use or disclosure of all private information in the bank's custody. There should be coverage not only for e-commerce and the bank's website, but for all customer and employee information stored off-line on the bank's network.
- Include a full policy limit for regulatory defense coverage for actions brought by regulators. "Duty to Defend" policies are preferable because cyber-insurers are typically experienced in privacy regulation and computer forensics.
- Cover third-party claims that occur worldwide. With its website, the bank's internal systems are "borderless" and claims can originate from anywhere in the world.

Ask your insurance agent to review your overall insurance program to determine if there are gaps in coverage. In this dynamic world of e-commerce, banks should work closely with their agents to put the right coverages in place.

¹⁾ "Bernanke Falls Victim to ID Theft After Wife's Purse Stolen", Associated Press, August 27, 2009

²⁾ "2008 ICBA Community Bank Technology Survey Results", www.ICBA.com, October 2008

³⁾ "New Exam Focus? Well-Capitalized Banks Hit with C&Ds Over IT Issues", www.FinCriAdvisor.com, November 15, 2009

⁴⁾ "Get Ready for Remote Capture Risk Management Scrutiny", www.SearchFinancialSecurity.com, October 5, 2009

⁵⁾ "Data Breach Lawsuit Puts Spotlight on Bank's Security Measures", www.SearchFinancialSecurity.com, October 8, 2009

⁶⁾ "Banks Liable for Cyber Criminals?", www.Blogs.finlaw.com/technologist, September 29, 2009

Kevin Rankin is an underwriter with CNA in the Community Bank group. He can be reached at kevin.rankin@cna.com or 312-822-4380.



The purpose of this article is to provide information, rather than advice or opinion. It is accurate to the best of the author's knowledge as of the date of the article. Accordingly, this article should not be viewed as a substitute for the guidance and recommendations of a retained professional. In addition, CNA does not endorse any coverages, systems, processes or protocols addressed herein unless they are produced or created by CNA. Any references to non-CNA Web sites are provided solely for convenience, and CNA disclaims any responsibility with respect to such Web sites.

To the extent this article contains any examples, please note that they are for illustrative purposes only and any similarity to actual individuals, entities, places or situations is unintentional and purely coincidental. In addition, any examples are not intended to establish any standards of care, to serve as legal advice appropriate for any particular factual situations, or to provide an acknowledgement that any given factual situation is covered under any CNA insurance policy. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All CNA products and services may not be available in all states and may be subject to change without notice.

11/09