

# Community Banks

## Customer Data: Threatened From Inside and Out

By Kevin Rankin, CNA Insurance

As the national recession deepens, cyber-crime is on the rise and crooks are becoming increasingly brazen and sophisticated. Additionally, rogue or disenchanting employees can sell customer data for fraudulent purposes and personal gain. Customer data is one of a community bank's most important assets. But most banks still rely on old-school Bankers Blanket Bonds or general liability policies, which were not designed to protect against this new generation of cyber risks.

The FBI's Internet Crime Complaint Center found that online crimes hit a record high of 275,000 complaints in 2008 (up 33% from 2007), amounting to \$265 million in losses (up from \$240 million in 2007).<sup>1)</sup> Until recently, cyber-attacks were simple solicitations indiscriminately transmitted to thousands of e-mail addresses at the same time. Now, however, criminals use detailed research to conduct "spear phishing" campaigns on specific individuals or businesses. In these well-orchestrated attacks, crooks send personalized e-mails to bank customers or set up fake bank websites complete with logos. Malicious cell phone text messages alert customers their bank debit cards have been deactivated and suggest they call back and leave personal information. Further, in an audacious scheme, thieves rigged ATMs of a New York bank to "skim" customer account and password information, going so far as to use hidden cameras to film customers entering their PIN numbers. The bank is reimbursing customers for their losses.<sup>2)</sup>

But while banks may have controls in place to keep criminals out, data theft can also be an inside job. The non-profit Identity Theft Resource Center (ITRC) found insider theft in 2008 accounted for almost 16% of breaches.<sup>3)</sup> The breaches are not limited to the large regional banks. Earlier this year, a bank in North Carolina discovered a former employee, with access to customer accounts, had sold bank customer information to outsiders. The former mailroom supervisor of a San Francisco bank had opened customer mail and sold the commercial and personal data as part of a large identity theft scam.

Conventional first party insurance coverages were designed to protect "tangible" property, such as money or securities, from named perils like robbery or fire. However, crucial customer and employee personal data such as Social Security Numbers, account information, or passwords is considered "intangible" property and typically would be excluded from traditional insurance coverages.

To address these potential gaps in coverage, the insurance industry has developed a variety of cyber insurance products. But these products vary greatly and buyers should consider which best fits their bank's needs.

Factors, buyers should consider include:

- Banks have a custodial duty to protect "any and all" private and confidential information, including that of employees, in their possession. Some policies limit coverage to only on-line activities. However, more than 68% of identity thefts involve offline (hard copy) records.<sup>4)</sup> Ensure your policy responds to breaches of both on-line and off-line data, both by outsiders and rogue employees.

- If your bank is the victim of a breach, notifying customers and complying with privacy laws can be expensive and time-consuming. Forty-five states now have customer notification laws in place. Additionally, later this year, new federal regulations (the “Red Flag Rules”) will require improved procedures for detecting and identifying identify theft. Cyber polices should provide “Duty to Notify” compliance cost with no or low deductibles. Coverage should be triggered not only by statutory duty, but rather by any incident that could harm the bank’s reputation. Your policy should also provide coverage for credit monitoring for affected customers and hiring a public relations firm to help restore the bank’s reputation.
- With its website, the bank’s internal systems are “borderless” and claims can originate from anywhere in the world. Be sure the cyber policy covers third party claims that can occur worldwide.
- Since lost or stolen media account for almost 50% of data compromises <sup>5)</sup>, make sure the policy covers losses resulting from all removable media, such as bank-owned laptops, PDAs, thumb drives, or even paper records, from any location, either from the office or on the road.
- Privacy violations are complex and expensive to defend, so inquire about policies in which the insurer has a duty, not just a right, to defend. Cyber insurers are typically experienced in privacy regulation and computer forensics.
- Since many banks outsource data processing, a cyber policy that protects against third party liability exposure it preferable. Also, the bank should have “hold harmless agreements”/“indemnification agreements” in place with their third party provider.

Ask your insurance agent to review your overall insurance program to determine if there are significant gaps in coverage. In these challenging economic times, banks should work closely with their agents to put the right coverage in place.

<sup>1)</sup> [www.ic3.gov/media/2009/090331.aspx](http://www.ic3.gov/media/2009/090331.aspx)

<sup>2)</sup> “Identity Theft Resource Center, 2009 Breach List”

<sup>3)</sup> [http://www.idtheftcenter.org/artman2/publish/m\\_press/2008\\_Data\\_Breach\\_Totals\\_Soar.shtml](http://www.idtheftcenter.org/artman2/publish/m_press/2008_Data_Breach_Totals_Soar.shtml)

<sup>4)</sup> “2005 Identity Fraud Survey Report.” January 26, 2005. Better Business Bureau and Javelin Strategy and research. Accessed July 26, 2007.

<sup>5)</sup> “How Many Identity Theft Victims Are There?” Privacy Rights Clearing House June 2007

*Kevin Rankin is an underwriter with CNA in the Community Bank group. He can be reached at [kevin.rankin@cna.com](mailto: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.

5/09