# PRIVACY NOTIFICATION

by Steve Brown

Everyone expects financial institutions to keep certain information confidential, but employees (and even management) can get caught up in the daily grind and sometimes let down their guard. As an industry, we need to be diligent, since studies show 16% of ID theft breaches were the result of employees. Safeguarding nonpublic information (NPI) is everyone's job so having a good program is critical.

Banking regulators define "customer information" as any record, whether in paper, electronic, or other form, containing NPI of a customer. That is pretty comprehensive, but it highlights areas bank programs must cover to be effective. As a reminder, NPI is personally identifiable financial information, but it does not include publicly available information. Employees do not need to be concerned if they drop annual financial statements somewhere, if their bank puts such statements on its web site.

To simplify what is NPI and what is not; try thinking of it as a simple math problem (A + B = NPI). To be NPI, the information must contain "A" (customer name, address or phone number) + "B" (a social security number, drivers license number, credit card number, account number/PIN or password). So, if you are in possession of a customer name + a social security number, you are in possession of NPI. Know also that having multiple "A" items or multiple "B" items (without an A AND B) is not NPI.

Now that we have identified what NPI is, we must protect it. This requires a written information security program, designed to ensure security / confidentiality of customer information, protect against threats to the information and with controls in place to protect against unauthorized access. Banks also must have policies, procedures, training, testing, technical and physical safeguards to protect NPI. Finally, banks must provide a report at least annually on customer privacy to the board of directors.

We don't have to tell bankers that examination teams are very serious about protecting customer information. At a minimum, regulators want banks to have a written information security program / policy that has been approved by the board. They will also want to see that the program is appropriate given the size and complexity of the bank, clearly states its objectives, assigns responsibility and provides methods for compliance / enforcement. In addition, examiners will review how often the bank updates its program to capture changes in systems / operations and whether it is adjusting to shifting risks.

In an effort to help bankers get ready for the next exam, we suggest creating a punch list that includes such items as identifying locations, systems and methods for storing, processing, transmitting and disposing of customer information. Identifying internal / external threats and ensuring risk management processes include controls to prevent unauthorized access to computer systems. Employees should also be prevented from providing NPI to unauthorized individuals, access should be controlled at physical locations, data should be encrypted / controlled and reported. In addition, duties should be segregated wherever NPI is handled, employee background checks should be conducted and systems should be closely monitored. Finally, banks should have a detailed

response program in place to specify actions to be taken whenever data has been compromised. Doing each of these will help the bank in its preparations.

Protecting NPI requires extra steps and diligence for everyone at the bank, but we like to think of this process as protecting our own information / identity. When we do that, it doesn't seem nearly as onerous and it gets people thinking about controlling the risk more consistently. Adding shredders around the bank, having a clean desk policy, locking doors / cabinets, hitting "Ctrl-Alt-Del" on the computer keyboard when you leave, doing background checks and other simple things can go a long way to protecting NPI. We'll delve into this topic again, but stay positive and spread the word that protecting NPI is everyone's job.

## BANK NEWS

**TARP Update**

The grapevine seems to indicate a term sheet for Subchapter S banks to get TARP may be coming shortly. We'll keep our eyes and ears open and keep you posted when we see something.

**Economic Forecast**

A group of Blue Chip economists predicts a weak recovery will not surface until late 2009 and unemployment will continue to rise into early 2010. The group predicts the recession will be the longest since World War II.

**Corporate Stress**

S&P indicates Q4 was the worst one on record (since 1956), as 444% more companies decreased their dividends.

**CRE Pressure**

elinquencies on commercial properties jumped from 1.5% at the end of 2007 to 2.2% as of the 3Q, a 46% increase. The rate is expected to rise to 3% by year-end.

**Nonperforming Loans**

S&P projects nonperforming loans at banks will continue to rise through 2010, reducing bank earnings, requiring increased loan loss reserves and weakening capital levels.

**Risk Ahead**

Banks that purchased and currently hold trust preferred securities in their investment portfolios are likely to face increased writedowns in coming quarters as the industry continues to deteriorate.