SAFEGUARDING SENSITIVE DATA

by Steve Brown

Every so often, under a program we have to ensure sensitive information is being safeguarded in desk areas, our Chief Risk Officer (CRO) and Chief Information Officer (CIO) will take a stroll around the office after hours. Their goal is to identify sensitive data left out so employee awareness is raised and everyone understands that a breach of confidential information could trigger either a monetary loss or one of reputation.

Since this program began, we have found ourselves standing at the door to the office and looking back at the desk and questioning: is there anything confidential in that stack of paper? Are the drawers locked? Have we left the key in the drawer? What is that coffee cup doing there? While we do not yet have fines in place for those who leave confidential data behind, we are working towards incorporating protection of data into employee evaluation forms.

As you stand at your own door tonight and scan the desk, ask yourself whether it contains loan files, audit reports, non-public financial data, policy documents, board of director documents or anything else that could be considered confidential and take steps to protect it.

We are constantly reminded by our CRO and CIO that executives, managers and employees all have the responsibility to ensure confidential information is locked up and away from casual view each and every day. Additional staff training, re-keying cabinets so they can lock, shredding sensitive material and purging unneeded files to make room for current work are all options to consider.

It is important to make the distinction that whenever you are working with confidential information, you also take on the responsibilities for protecting it. Given the sensitive nature of the information, an extra layer of care must be applied and awareness must be increased.

Some tips to follow for different types of data sources include: Electronic: Never disclose personal authentication information such as a user ID or password; keep security software patches up to date; ensure antivirus software is working; do not leave computers unattended if you can avoid it; make sure portable storage devices, such as USB drives, are locked away; do not open email attachments of any sort if you cannot identify the sender; make sure you have a secure connection if accessing data through the web; and periodically close the browser to start a new session (eliminates hackers from accessing information stored in browser cookies). Physical: Keep your computer monitor positioned so it cannot be easily seen by others when you are reviewing sensitive data; lock your desk drawers; lock your office door; log out of the computer whenever you walk away; and occasionally change keys, passwords, locks, etc. to ensure access remains limited to only authorized personnel.

Finally, banks should be sure to implement standards and practices that protect sensitive data throughout the company. These should include having strong policies and procedures that are regularly updated; properly maintaining systems that contain or transmit sensitive information; periodically conducting background checks on people with access to confidential data or systems; notifying the CRO/CIO when new systems will contain or have access to sensitive data; and maintain

well defined functions and approved authorizations for employees who might access confidential data.

Now, if we could only remember where we left that folder that contains the bank account number, social security number, tax return, cancelled checks, credit card numbers, name and bank...

BANK NEWS

FDIC Special Assessment

The final ruling is expected to be out this Friday. While the assessment for additional insurance is at 20bp, it is expected to go to at least 10bp. The optimists amongst us are hoping for something lower - or at least a reduction in future years.

No Extension For Debt

The FDIC has decided it will not extend TLGP to 10Ys, after reportedly receiving pushback from the Treasury. The FDIC was considering extending the program from its current 3Y term, but worries have increased that banks may be leaning too much on this as a source for funding as of late. Since inception, banks have issued $343B in debt under TLGP and program guarantees about $1T in business checking account deposits.

Beneift of Change

The recent accounting change that allows companies to separate declines in securities value (between the credit portion and the portion driven by distressed market conditions) has allowed most FHLBs in the 1Q to avoid taking hits to earnings due to ongoing writedowns on private label mortgages (because they were holding these securities to maturity).

TARP Boost

A Treasury report released on Friday shows the total number of loans at the 21 largest TARP recipients jumped 27% in Mar. compared to Feb. Lending activity improved across the board, however the appetite for new loans has fallen and demand for commercial real estate and business loans fell further during the month.

Out Perhaps

CNBC is reporting that both Goldman Sachs and JPMorgan have been given approval to exit TARP.