

# Supervisory Spotlight

A Regulator's Perspective on Issues Facing Western Banks

Banking Supervision & Regulation  
Federal Reserve Bank of San Francisco

May 2014



Greetings!

We recently held our Division's semiannual Risk Assessment Session, where we discussed a variety of risks that challenge our Twelfth District bankers. It probably isn't a surprise to you that one of the top three risks facing community bankers in our district is information security, and particularly cybersecurity. I know that I cannot open a newspaper, surf the web, or turn on the TV without seeing breaking news about cyberattacks and cyber threats.

As bank regulators, we believe that the growing sophistication and volume of cyber threats present a serious risk to all financial institutions, including community institutions. To coordinate and raise awareness on this important issue, the Federal Financial Institutions Examination Council (FFIEC) created the Cybersecurity and Critical Infrastructure Working Group.

On April 2, the FFIEC issued a [statement](#) to notify financial institutions of the risks associated with cyberattacks on Automated Teller Machine (ATM) and card authorization systems and the continued distributed denial of service (DDoS) attacks on public-facing websites. On April 10, the FFIEC issued a separate [statement](#) on expectations for financial institutions to address the "Heartbleed" vulnerability. I hope that you have had an opportunity to discuss these risks with your internal and outsourced IT professionals and are taking the appropriate steps to protect your institutions.

But these FFIEC releases cover just the tip of the cyber threat iceberg. I'm sure that staying on top of the increasing number of cyber risks and the volume of new cyber information is a formidable task for community bankers, most of whom rely on third parties for much of their technology services. While it is critical that your internal and outsourced systems remain secure, there is a host of technological and regulatory guidance on how to do just that, so I won't discuss that here.

However, just as critical for community bank leadership is the ability to step back and understand the true scope of cyber threats that may affect their institution and to develop risk management responses that are appropriate for their infrastructure, customer base, products, and services. Toward that end, the FFIEC is offering a webinar on May 7, 2014, at 10:00 am Pacific entitled, *Ask the Regulators: What Today's CEO Needs To Know About the Threats They Don't See*. This program will feature speakers from the three federal banking agencies, the NCUA, and the Texas Department of Banking. A representative from the [Financial Services – Information Sharing and Analysis Center \(FS-ISAC\)](#), an industry forum for collaboration on critical security threats facing the global financial services sector, will discuss their information sharing and education initiatives. The Federal Reserve is offering registration to this webinar through its [Ask the Fed](#) program, and I encourage you and your leadership team to make every effort to participate.

While you focus on threat identification, risk management, and the related technological solutions, it is important to remember that fixing one of the weakest links in your information security chain may not require a technological fix. Educating your customers about the steps that they can and must take to protect their personal information will go a long way toward reducing the vulnerable points of entry into your systems. As noted in the Community Banking Connections article, [Staying Ahead of Fraudsters: Protecting Your Bank and Your Customers from Payments Fraud](#), institutions responding to a Federal Reserve survey identified consumer education as one of the top three fraud prevention techniques. In this new age of increased use of cyberbanking and the commensurate increase in cyberattacks, you can help your customers help themselves and your bank by encouraging them to:

- ◆ use unique passwords for their online accounts and for their mobile devices
- ◆ change their passwords regularly
- ◆ check their account transactions regularly
- ◆ shred documents and receipts
- ◆ use skepticism when receiving an unsolicited phone or email contact about their account

As always, I appreciate feedback and suggestions for topics that are of particular concern to your institutions.

Best regards,

*Teresa Curran*

Teresa.Curran@sf.frb.org

## Resources

You can view additional Community Banking Connections articles and subscribe to an electronic or hard copy of the publication at <http://www.communitybankingconnections.org/>. You can also view additional Consumer Compliance Outlook articles and subscribe to that publication at <http://www.philadelphiafed.org/bank-resources/publications/consumer-compliance-outlook/>. Please also consider subscribing to receive notifications of our Reserve Bank's Banking Supervision publications and programs at <http://www.frbsf.org/our-district/subscriptions/banking-supervision-regulation-subscriptions/>.