Bank Safety & Soundness Advisor

Executive intelligence on bank exams, enforcement and risk management.

July 18, 2011

FFIEC Expands, Intensifies Standards for Internet Security

Six years is a lifetime in internet fraud. Back in 2005, when the FFIEC last released guidance to banks on internet banking security, hackers were all busy phishing for individual account passwords and credit card numbers and bankers were, in large part, treating internet fraud as a compliance issue. Since then, the scale, frequency and sophistication of cyber attacks have all exploded and the stakes are significantly higher. A breach today can involve thousands of accounts and cost millions to fix. In response to the radically changed threat environment, the FFIEC released new electronic banking fraud guidance last month. The new guidance may be late in coming, but it's more detailed, more proscriptive and improves significantly on its 2005 predecessor, experts say.

The guidance needed an update, says Terry Austin, CEO of internet security firm Guardian Analytics, Los Altos, Calif. Too much has changed in internet fraud and fraud prevention since the original 2005 guidance.

"The guidance has been long overdue," he says. "Criminal technology has outpaced the [2005] guidelines. The market's

See Page 6

Even with Good Internet Security, Poor Customer Education Can Still Lead to Liability, Risk

In late 2009, an employee of Experi-Metal, a Michigan-based supplier and manufacturer of prototype tooling, received an e-mail that did not come from his company's bank, Comerica ($54 billion), Dallas. Unfortunately for him, his company and the bank, he thought it did. The employee clicked the link and arrived at a dummy site where he then provided internet scammers with his company's confidential bank account information. The scammers quickly initiated $1.9 million in fraudulent transfers.

This all took place outside the bank's security apparatus. Bank security didn't fail. Comerica felt it did nothing wrong. Nevertheless, the bank found itself in court – Experi-Metal alleged that the bank allowed tens of wire transactions to go through after the bank knew that fraudulent transfers had already gone through – and with its name all over the papers. Earlier this month, Experi-Metal won its suit against Comerica,

(continued on page 2)

Examiners Won't Second Guess "Reasonable" Appraisals, OCC Says

Plunging real estate values precipitated the recession and markets are still plenty murky, so it's not surprising that examiners and banks have argued – and continue to argue – over property appraisals. Differences in opinion over property values have been one of the most controversial aspects of bank exams in the last few years. Many banks contend that examiners are routinely and inappropriately second guessing appraisals from banks and their appraisers. Is this regulatory overreach? It may depend on your definition of overreach.

Last week, Jennifer Kelly, the OCC's Senior Deputy Comptroller for Midsize and Community Banks, weighed in on the subject midway through her Congressional Testimony. Agency examiners do "adjust" appraisals, the official admits, though the agency has "taken steps to minimize the need for such adjustments during the current cycle." What's more, she adds, if banks got reasonable appraisals to begin with, they wouldn't need any adjustment.

"In 2008, in a nationwide teleconference and supervisory memo, we reiterated to examiners that it is management's responsibility to have

(continued on page 4)

SUBSCRIBER SERVICES

MISSION:

Bank Safety & Soundness Advisor provides independent, executive intelligence on bank exams, enforcement and risk management.

EDITORIAL:

Need us to investigate a topic? Want to express your opinion? Please call or e-mail us.

Publisher:

Aaron Steinberg
800-929-4824 ext 2471
asteinberg@banksoundness.com

Group Publisher:

Hugh Kennedy
800-929-4824 ext 2213
hkennedy@banksoundness.com

SUBSCRIPTIONS:

Direct questions about subscriptions to:

Phone: 1-877-320-7147;
Fax: 301-287-2945;
or send an **e-mail** to
Customer@banksoundness.com.

Published weekly (48 times a year).

Price: $595/yr.

EDITORIAL CONCERNS:

Our goal is to provide you with the most accurate and balanced information available anywhere. If you ever feel we're not living up to this standard, I want to know about it. Please call me, Hugh Kennedy, Group Publisher, direct at 1-800-929-4824 ext. 2213.

ADDRESS:

Bank Safety & Soundness Advisor
Two Washingtonian Center
9737 Washingtonian Blvd., Ste. 100
Gaithersburg, MD 20878-7364

Customer Ed

(continued from p. 1)

which is now on the hook for $561,000 in damages.

Banks can only safeguard so much by themselves. Fraudsters and hackers can beat an ironclad internet security system if bank customers are – however unwittingly – helping them out. And, as examples like Comerica show, security lapses outside the bank's security system can result in big financial and reputational risk. That's why for years, fraud prevention specialists have been pushing banks to educate customers on the full gamut of ways and means criminals have to tap their bank accounts through their computers and mobile phones.

It's clear now that the regulators agree. In recent FFIEC guidance on authentication in internet banking, financial regulators set standards for customer education for the first time. With the addition of the new guidance and in the wake of the Comerica case, banks could be seeing expanded liability for customer-triggered breaches, which only makes internet security and customer education all the more important, experts say.

Even with a relatively small breach, banks will take a hit to their reputation, and that can be costly. That's why it is and has long been in a bank's best interest to educate their customers on internet security best practices, says Kevin Funnell, an attorney in the Frisco, Texas office of Bieging Shapiro & Burrus LLP.

"Thus far, the major security breaches involving banks, which have resulted in losses to customers and lawsuits being filed by those customers against their banks, have been caused by cybercrooks compromising the security of the customer's computer system due, in many cases, to some basic ignorance by customers in protecting the security of their systems," Funnell says. "Educating the customers about how better to protect themselves can prevent the breaches from occurring in the first place and can better protect the bank from liability to the customer if the customer is subsequently negligent notwithstanding the educational efforts of the bank. I think the major risk to banks thus far in these incidents has not been legal risk but reputational risk. It's not good for a bank's reputation to have a story in the local newspaper that thieves looted a customer's account through the bank's online banking system, regardless of the customer's fault."

For a number of reasons, many banks have been reluctant to educate their customers adequately or even at all, Funnell adds. Smaller banks, in particular, don't think they have the resources to spare on an education program. Another prevalent issue involves skittish bank counsel, many of whom worry not about data breaches, but rather about the additional legal risk a bank could be taking on when it tries to educate consumers but makes mistakes or omissions in doing so. Banks can't lean on these excuses anymore, Funnell says.

"Those problems all need to be dealt with, because the FFIEC says all banks need to start educating their customers, so no banks will be able to justify sticking their head in the sand in the future," he says.

Customer education make sense, but there are limits to its

efficacy, argues Reed Taussig, CEO of internet security firm ThreatMetrix, Los Altos, Calif.

"It is a good idea to make the customer aware [of electronic banking risk]," Austin says. "But if my 81-year-old mother-in-law's bank gave her instructions about how to make her computer safe, she'd be clueless. It's unrealistic to assume that all customers will be able to deploy complex solutions."

Nevertheless, what the new FFIEC guidelines are really pushing is not a foolproof solution to customer security lapses, but rather for greater transparency – and that transparency will only improve overall industry security, argues Terry Austin, CEO of internet security firm Guardian Analytics, Los Altos, Calif.

"The guidance is telling financial institutions to be more transparent," he says. "[Regulators] want banks to tell customers what the risks are and what their liabilities are. They want banks to tell customers what protection mechanisms are in place, in the event of fraud, and what consumers can do to protect themselves. The FFIEC is saying that banks need to have that transparency so consumers can make better decisions."

More transparency will push banks towards better, more secure systems and that will benefit banks, whether they're liable for the breach or not, he argues. Even if the bank doesn't have the liability, they'll still get the negative publicity.

"We've seen a lot of lawsuits in the last few years," he says. "[Companies that lost money in a breach] will sue and find, lo and behold, they've given up the right to be reimbursed. The bank may not be liable, but that's headline making news."

Even liability issues aren't quite so clear anymore. At least when it came to wire transfers and business customers, banks could count on avoiding liability as long as they adopted reasonable security procedures and the customers signed off on them, says Andrew Lorentz, a partner with Davis Wright Tremaine LLP in Washington, D.C.

"[Regulators] want banks to tell customers what the risks are and what their liabilities are."

"Under state law 4A of the U.C.C. [Uniform Commercial Code], there is a concept of commercially reasonable security procedures," says Lorentz. "If a bank proposes reasonable security procedures, the customer accepts them, those processes are followed in connection with wire transfers, and an account is compromised through no fault of the bank, then the liability for fraud shifts to the customer."

When the court found Comerica liable, Experi-Metal v. Comerica upended that precedent. "The court latched on to a good faith argument regarding acceptance of the wires and used that as a way to impose liability," Lorentz says. "Whether that survives appeal, we don't know. But banks should be thinking about [cases like] this."

Another factor that may change the equilibrium for bank liability in security breaches: the FFIEC guidance itself. The arrival of new authentication guidance from the FFIEC may actually add to banks' legal risk, Lorentz argues. Lawyers can point to the expanded guidance to try to show how defendant banks fell short of the guidance's standards.

"There's a heightened, increased standard at the FFIEC for internet security now and I think that plaintiffs and their counsel may focus on that – on those details," he says. "They'll say, for example, that the bank's authentication process was inadequate."

No matter what happens with liability, precedent or the Comerica v. Experi-Metal case on appeal, however, banks might be better off focusing on the more significant issue: reputation risk. It doesn't ultimately matter if a bank has liability in a given situation or not; customers will always expect banks to safeguard the funds they put into a bank, whether it involves physically carrying cash or check to a bank branch or depositing funds to be used electronically, argues ThreatMatrix's Taussig. A bank can avoid liability in some cases, but whether it does or not, customers will view the bank as an institution that can't keep their money safe.

"In the Comerica case, the defense said: 'It was you, the consumer, who allowed the breach, not us so therefore it's your fault.' But if you think about it, when customers put money into a bank, they're handing over an asset and they expect the bank to be the custodian of that asset," Taussig says. "Customers want the bank to keep that asset safe. I think that banks have a real economic and moral responsibility to look at this the same way." ■

Appraisals

(continued from p. 1)

updated borrower information and current real estate appraisals," Kelly said. "We also noted that a new appraisal may not be necessary in instances where an internal evaluation by the bank appropriately updates the original appraisal assumptions to reflect current market conditions and provides an estimate of the collateral's fair value for impairment analysis."

As far as agency policy is concerned, examiners should defer to quality appraisals, she said. "As noted in the October 2009 CRE policy statement, appropriately supported assumptions are to be given a reasonable degree of deference by examiners. Provided that the appraisal is reasonable, our examiners will not make adjustments or apply an additional haircut to the collateral."

An informal poll of *BSSA* subscribers finds that nearly 65% of banks have experienced appraisal second-guessing by the examiners.

"They basically don't believe [the appraisal] or criticize all appraisals," said one bank official of his FDIC examiners. "Consistency might be a problem. On a three-way participation loan on land development, our bank got written up by FDIC on the value we used in the appraisal. The lead bank was examined two weeks later by FDIC with no issue, and our sister bank located in Ky. was examined a few months after that by state examiners with no issue cited."

Examiners are expecting adjusted values every quarter, said another official. A third banker's experience reinforced the notion. "[Examiners] said that an appraisal that was 6-to-twelve months old was not acceptable because the market had obviously deteriorated in that period," the official said. "There were no facts behind the statement. We had it reappraised at considerable cost and the original value was supported."

"They basically don't believe [the appraisal] or criticize all appraisals."

On Loan Classification, Cash Flow, Collateral and Capital

The OCC's Kelly also addressed a few other high-volume examiner criticisms she and her colleagues hear from banks in regards to exams.

Concern: Examiners are barring loans to certain borrowers or industries, or are criticizing loans simply because they are located in a state with a high mortgage foreclosure rate or to an industry experiencing problems.

Response: No we don't.

Yes, banks need quality underwriting, need to manage their own risk and monitor the bank's exposure to an individual or industry segment, Kelly said. Banks also have to run stress scenarios to test borrowers' or industries' capacity to uphold their loan obligations. Nevertheless, she adds, examiners won't simply blacklist borrowers or industries.

"[E]xaminers do not criticize loans simply because a borrower is located in a certain geographic region or operates in a certain industry," she said. "Each loan must be evaluated based on its own structure, terms, and the borrower's willingness and ability to repay the loan under reasonable terms. Market conditions, however, can influence a borrower's repayment prospects and the cash flow potential of the business operations or underlying collateral, and these are factors that we expect bank management to consider when evaluating a loan."

Concern: Examiners prevent banks from working with a given borrower simply because the examiner classified that borrower's loan.

Response: We don't do that either.

The OCC expects banks to classify a loan when a borrower's ability to repay deteriorates, but that shouldn't impact the bank's willingness or ability to work with the borrower, Kelly said.

"Although some bankers may infer that they are no longer allowed to extend credit to borrowers whose loans have been classified, this is simply not the OCC's position," she adds. "We expect and, in fact, encourage bankers to continue working with 'classified' borrowers who are viable. An increase in classified loans does not automatically trigger supervisory action – we expect banks to have higher classified loan ratios during economic downturns – provided that bank management is being realistic in its assessments, has reasonable workout plans, and is maintaining adequate loan loss reserves and capital ratios."

Concern: Examiners encounter loans to borrowers who are current and can meet their debt obligation – and classify them anyway.

Response: Okay, we sometimes do this, but not without good reason.

"The OCC does not direct banks to classify borrowers that have the demonstrated ability to service both interest and principal under reasonable payment schedules, [but] there are instances where liberal underwriting structures can mask credit weaknesses that jeopardize repayment of the loan," Kelly said.

Kelly points to what she considers a common example: bank-funded interest reserves on CRE projects where expected leases or sales fall below projections and property values have declined. "In these cases, examiners will not just accept that the loan is good quality because it is current; instead, they will also evaluate the borrower's ability to repay the debt within a reasonable timeframe," she adds.

Concern: Examiners criticize loans or borrowers simply because the current market value of their collateral has declined and then force bankers to write down loans to current distressed market values.

Response: If the property behind the loan has inadequate cash flow and the only potential source of repayment is the collateral, then yes, we'll do it.

Examiners won't write down loans just because the value of the underlying collateral slumped below the loan balance, but that doesn't mean that examiners won't do it, Kelly said. "For many CRE projects, the value of the collateral and the repayment of the loan are both dependent on the cash flows that the underlying project is expected to generate. Because of this linkage, current collateral values can be an important indicator of the project's viability and can signal changes that will adversely affect the cash flow available to service or repay the loan."

When examiners make write-down decisions, they should consider the adequacy of cash flow available to service debt, including cash flow from the collateral, support from guarantors or other sources, she said. But if those sources aren't there and collateral is all that's left, "examiners will direct the bank to write down the loan balances to the value of the collateral, less estimated costs to sell," she adds.

Examiners won't write down loans just because the value of the underlying collateral slumped below the loan balance, but that doesn't mean that examiners won't do it.

Concern: Examiners are penalizing loan modifications by aggressively placing loans on nonaccrual status following a modification, even though the borrower has demonstrated a pattern of making contractual principal and interest payments under the loan's modified terms.

Response: It's GAAP's world; We're all just living in it.

Interest income criteria in GAAP determine a loan's accrual status, Kelly said. "For a loan that has been modified, if the borrower has demonstrated performance under the previous terms and shows the capacity to continue to perform under the restructured terms, the loan will likely remain on accrual. If the borrower was materially delinquent on payments prior to the restructure, but shows potential capacity to meet the restructured terms, the loan would likely remain on nonaccrual until the borrower has demonstrated a reasonable period of performance."

Concern: Examiners are arbitrarily applying de facto higher regulatory capital requirements that constrain banks' ability to lend.

Response: The regulatory standard is the bare minimum. Banks with some risk concentrations should expect examiners to demand more capital.

The OCC, concerned about credit loss in recent years, has absolutely been asking banks to beef up loan loss reserves and capital cushions, she says. And also, she adds, the agency is not enamored with banks that sit right at or just above the regulatory capital standards, either.

"Indeed, if a bank simply maintained its capital at the minimum level defined by regulation and then incurred unexpected losses, the resulting decline in its capital ratios would immediately trigger the provisions of Prompt Corrective Action that would constrain the bank's activities," she said. "Thus, there are instances where we have directed, and will direct, bank management to maintain higher capital buffers if they choose to have significant risk concentrations. Such decisions, however, are not made unilaterally by a field examiner. Any such directive is reviewed and approved by our district supervision management teams." ■

FFIEC

(continued from p. 1)

moved on and the technology has changed. It's good the guidance is out – it's a much stronger framework for financial institutions to know what's expected of them."

Bankers could have used better guidance some years ago and this new version does have some notable holes – it doesn't address mobile banking, for example. But at least what the regulators put out gives banks solid advice and requirements they can use to address internet fraud right now, adds Julie McNelley, a senior analyst and internet fraud expert at Aité Group, Boston.

"I think that if we'd waited for the perfect guidance, we'd be waiting at least another two years," adds McNelley. "But, this one is two years too late. The threat environment has drastically changed and some financial institutions haven't changed what they've been doing in response."

The new guidance instructs banks to make changes to their internet security systems, such as the additions of layered security and processes designed to detect anomalous activities. It also addresses consumer education and pushes a risk-based method for constructing a fraud prevention mechanism.

"The 2005 guidance was so high-level and nebulous," McNelley says. "It didn't give you a roadmap or mandate any kind of infrastructure for financial institutions to look to – to make sure theirs was up to snuff. It confused a lot of people. The new guidance does a good job of saying: 'You need layered security.' For those financial institutions who met the 2005 standard and called it a day for six years running, that's not good enough."

How is the guidance more prescriptive? McNelley points to one notable example: the guidance not only requires a periodic review, but it also defines it. Financial institutions should survey the new information in security and update their exiting risk assessments prior to implementing new electronic services at least once every 12 months.

Requirements

According to the FFIEC guidance, banks will now be expected to:

- Build security systems that do not rely on any single control for authorizing high risk transactions. The FFIEC now requires layered security;
- Monitor and review controls at least once every twelve months;
- Design their internet security apparatus according to risk-based principles. I.e., if a given internet product involves higher risk, it should get more thorough protection;
- Offer multifactor authentication to business customers; and
- Include in their security mechanism two elements: a process designed to detect and respond to anomalies and enhanced controls for system administrators. ■

Not All Layered Security Elements Equal (or Interchangeable)

Security experts contacted by *BSSA* lauded the FFIEC for insisting on layered security programs for banks. Nevertheless, banks should be careful how they implement this particular section of the guidance, says Julie McNelley, a senior analyst and internet fraud expert at Aité Group, Boston.

The concept behind layered security is that banks should use multiple, overlapping elements in their security mechanism as a method for minimizing weaknesses in any single element. It's the right idea, says McNelley, but the guidance, which simply states the need for layered security and then provides a list of options, suggests that banks can pick a few at random and be set. Actually, those layered security plans need to be designed because those elements need to complement one another, McNelley says.

"The guidance gives a long list of potential layered technologies, but it didn't explain how those technologies work together," she says. "It doesn't discuss what risks or weaknesses they address. Unless a financial institution really does its homework, it could pick some off the list and find themselves protected against ABC threats, but not XYZ." ■