

INVICTUS

Bank Insights

Pre-Filing Make Sense in M&A Deals

Want smoother sailing for your merger or acquisition? Then make sure your bank goes through a pre-filing review to get regulatory feedback on the application, the Federal Reserve suggests in its **latest report** on banking applications.

“Processing delays can be avoided by using the pre-filing process, which provides applicants the opportunity to work with Federal Reserve staff to receive critical feedback on potential issues related to acquisitions or other proposals before filing a formal application,” the report notes.

The Fed made clear in **2012 guidance** that community banks could shorten the M&A review period by going through an optional pre-approval screening. The Fed said its staff will respond to all pre-filing requests within 60 days.

Among items that the Fed can review are “draft transactional and structural documents such as shareholder agreements, purchase agreements, voting agreements, side letters, offering documents, partnership agreements, or qualified family partnership agreements. In addition, pre-filings may include questions regarding the type of filing required, if any; the individuals or entities that would need to join a filing; and whether an entity would be considered to be a “company” or have “control” under the Bank Holding Company Act or the Home Owners’ Loan Act,” its guidance notes.

The Fed reported M&A proposals have accounted for about 15 to 20 percent of total approved proposals over the past four years. Before approving such deals, the Fed says it considers “the applicant’s current and pro forma financial condition and future prospects, managerial resources, consumer compliance record and performance under the CRA and the Bank Secrecy Act/anti-money-laundering compliance programs, public benefits, and the competitive and financial stability effects of the proposal,” as well as ownership changes and Fed policy questions.

Community banks with assets between \$1 billion and \$10 billion saw a sharp increase in the number of bank mergers, with 82 deals approved in 2014 compared with 44 in 2013, the Fed reported. The Fed said it approved 131 M&A deals for smaller community banks (assets of less than \$1 billion) in 2014 compared with 128 in 2013.

On average, the larger community bank M&A deals took 68 days to go through the final approval process, while the smaller deals took 52 days. The statistics also reveal that adverse public comments about a bank application will significantly lengthen the time it takes for approval; those proposals with negative public input took on average 206 days for approval, while those without took on average about 60 days.

Pre-Filing ‘Very Useful’ to Community Banks

The Fed says its pre-filing process is especially useful to community banks. Each application is allowed just one pre-filing review. Although optional, the process allows banks to get critical feedback before a formal application is filed. The process:

- Is not part of the formal review period for applications
- Won’t identify all issues or concerns
- May not be predictive of the final outcome

The Fed revealed that 52 proposals were withdrawn in the second half of 2014, 17 after consultation with staff. While the official feedback won’t resolve every issue with a bank application – or guarantee approval – banking experts say there are many reasons why the pre-filing process is a smart move. Here are some guidelines:

- Be sure that your board understands how an M&A deal will affect your regulatory capital going forward. Be ready to demonstrate the impact to regulators in the pre-approval review, not only on your own bank, but on the combined entity going forward, recommends Invictus Consulting Group Chairman Kamal Mustafa.
- Position your acquisition as a solution to a problem, Mustafa advises. That will help focus the conversations in the pre-filing stage, and show why the transaction is necessary for the bank’s strategic objectives. Tailor your final application to address regulatory concerns uncovered in the pre-approval process.
- Have a pre-announcement regulatory strategy. Balance the risks of meeting with regulators too early in the process when you might not have answers to all their questions with the potential costs and delays that could happen if you start the conversation too late, advises the law firm of Skadden Arps in **“Managing Regulatory Risk in Bank M&A”**.
- Getting an accurate read on how regulators will react to your deal is crucial, **advises the law firm** of

Inside this issue:

- As Cyber Threats Increase, Regulators Worry about Bank Readiness (page 2)
- Is Your Bank on Top of Cybersecurity (page 3)
- Failing to Plan is Planning to Fail (page 4)

Wachtell, Lipton, Rosen & Katz . “Potential acquirers should expect greater pre-signing consultation with regulators and should expect to be required to provide more rigorous and refined information than in the past.” Be prepared to present detailed pro forma information and business plans, the law firm suggests.

- Regulators expect to be part of the conversation early, **advises the law firm** of Sullivan & Cromwell LLP. The firm advises its clients to “engage in a proactive and regular dialogue with their bank regulators regarding strategic acquisition plans and the viability of such plans, regardless of whether they have any specific acquisition targets in mind.” When there is a specific target, the bank should vet the plan “well in advance of any proposed transaction announcement” with as much key information as possible. ■

As Cyber Threats Increase, Regulators Worry about Bank Readiness

Don’t think a community bank is immune from cyber attacks. Regulators are increasingly focused on cybersecurity and expect your bank to be on top of threats, including those that may hit your third-party service providers. In today’s interconnected world, banks need to protect their data, websites, apps and internal network.

“Cyber attacks have increased in frequency and severity over the past two years. The attacks often involve the theft of credentials used by customers, employees, and third parties to authenticate themselves when accessing business applications and systems,” the Federal Financial Institutions Examination Council warned in late March.

“Cyber criminals can use stolen credentials to commit fraud or identity theft, modify and disrupt information systems, and obtain, destroy, or corrupt data. Also, cyber criminals often introduce malware to business systems through e-mail attachments, connecting infected external devices, such as USB drives, to computers or networks, or by introducing the malware directly onto the business systems using compromised credentials,” the FFIEC wrote.

Community banks should make sure they test their incident response and business continuity plans and know what to do if their bank – or a third-party provider – is attacked, the regulators warned. Banks should have a plan to make sure that recovery strategies reflect the potential for a simultaneous attack on both the bank and its backup data center.

New York State last year said it was pumping up its IT exams to focus on cybersecurity readiness. It wants all institutions to view cybersecurity as “an integral part of their overall risk

Cybersecurity Expectations for Banks

The FFIEC says each bank should:

- **Securely configure systems and services**
- **Review, update, and test incident response and business continuity plans**
- **Conduct ongoing information security risk assessments**
- **Perform security monitoring, prevention, and risk mitigation**
- **Protect against unauthorized access**
- **Implement and test controls around critical systems regularly**
- **Enhance information security awareness and training programs**
- **Participate in industry information-sharing forums, such as the Financial Services Information Sharing and Analysis Center.**

management strategy, rather than solely as a subset of information technology,” state regulators **said in March**.

The new exams focus on whether banks have the proper corporate governance policies and procedures to manage cybersecurity issues and risks. Banks will be expected to demonstrate that they have the right reporting structure, resources, safeguards and testing to guard against an attack, and business continuity plans in place in case one happens. Federal regulators may follow suit.

The CEO and the board are responsible for cybersecurity management, the Conference of State Bank Supervisors stresses in a “Cybersecurity 101,” a **report** designed for community bank CEOs.

Here are some questions every CEO should ask to understand a bank’s risks, according to the guide:

1. Does my bank know what information it manages, where it is stored, how sensitive it is and who has access to it?
2. What are my bank’s key business information assets and are they adequately protected? Is confidential information – data that would severely impact the bank if lost, damaged or released-- treated like a crown jewel?
3. What types of internet connections does my bank have and how are they managed and protected? Does the bank allow employees to bring their own devices to work and if so, what controls are placed on that?
4. How is my bank connecting to third parties and ensuring they are managing their cybersecurity risks?

Once CEOs understand the answers to those questions, and classify their information assets to know their importance, they can then begin identifying the bank's threats and vulnerabilities. Regulators have encouraged community banks to join the **Financial Services Information and Analysis Center**.

New York state regulators **surveyed banks last year** and discovered that many banks were reluctant to reveal "perceived or actual security weaknesses to competitors," yet the most productive information-sharing must focus on specific threats and solutions. This is especially important to community banks, which have limited financial resources and must spend wisely to be the most effective. ■

Is Your Bank on Top of Cybersecurity?

By **Joe Oleksak**

Increasing use of online and mobile banking technologies has made banks and their customers more vulnerable than ever before. Given the huge cost of a data breach — in terms of both monetary loss and reputational damage — all banks should have a solid program for assessing and addressing cybersecurity risks.

The FFIEC has outlined the steps banks should take to address two severe threats: distributed denial-of-service (DDoS) attacks and cyberattacks on ATM and card authorization systems.

DDoS attacks on public websites slow website response times and otherwise disrupt network resources. They're designed to prevent customers from accessing bank information and services and to interfere with back-office operations. In some cases, the FFIEC explained, criminals use DDoS attacks as a diversionary tactic in connection with attempts to initiate fraudulent wire or ACH transfers using stolen customer or bank employee credentials.

Banks should address DDoS readiness as part of their ongoing information security and incident response plans. In addition to evaluating the risks to critical systems, banks should:

- Monitor website traffic to detect attacks,
- Activate incident response plans as appropriate (including notification of Internet service providers and customers), and
- Consider sharing information with law enforcement and organizations, such as the Financial Services Information Sharing and Analysis Center.

Banks also should ensure sufficient staffing for the duration of an attack and consider engaging third-party service providers to manage Internet traffic flow. Following an attack, a bank must identify any gaps in its response and modify its risk management controls accordingly. Additionally, the board of directors should be informed.

The FFIEC also has warned about a dangerous form of ATM cash-out fraud known as "unlimited operations." It enables criminals to withdraw funds well beyond ATM control limits and even beyond the cash balance in customer accounts. In one recent attack, criminals used unlimited operations to steal more than \$40 million using only 12 debit card accounts.

Criminals typically send phishing emails to bank employees in an attempt to install malware on the bank's network, giving themselves the ability to alter the settings on web-based ATM control panels. By increasing or eliminating limits on ATM cash disbursements and reducing fraud and security-related controls, criminals can quickly withdraw significant sums using fraudulent debit or other ATM cards.

The FFIEC statement notes that banks may initially be liable for ATM fraud losses, even if they outsource their card-issuing function to a card processor and the compromise takes place at the processor.

To mitigate ATM fraud risks, banks should:

- Conduct ongoing information security risk assessments
- Perform security monitoring, prevention, and risk mitigation, including monitoring third-party processors and ATM transaction activity for unusual behavior
- Take steps to protect against unauthorized access
- Review — and periodically test — the adequacy of controls over IT networks, card authorization systems, ATM usage parameters, and fraud detection processes
- Conduct regular training programs
- Test incident response plans

Editor's Note: Joe Oleksak is a partner in information technology consulting at Plante Moran in Illinois. ■

Cyber Resources

Regulators recommend that banks use the following as resources:

- **Federal Trade Commission's On Guard Online**
- **National Cyber Security Alliance's Stay Safe Online**
- **US-Cert Security Tip (STI-003)
"Handling Destructive Malware"**
- **Joint Security Awareness Report (JSAR-12-241-01B)
"Shamoon/DstTrack Malware"**

Read Between the Lines

Each month *Bank Insights* reviews news from regulators and others to give perspective on regulatory challenges.

Gruenberg: Failing to Plan is Planning to Fail

Too many banks are reaching for yield, launching new products or business lines or looking for sources of non-interest income without adequate strategic planning, FDIC Chairman Martin J. Gruenberg **told** the American Association of Bank Directors.


“There’s an old saying that “failing to plan is planning to fail.” One of the important lessons we learned from the financial crisis is that poor planning can harm institutions, their communities, and the financial system as a whole,” he said. The FDIC expects banks to have sound strategic planning processes in place – not just “a piece of paper”—that measure actual versus planned results.

CFPB Request for Student Loan Info May Signal New Rules

 The Consumer Financial Protection Bureau is asking the public to share their student loan **servicing stories** – and that may be a sign that reform is on the way. The bureau says it will use the info “to assist market participants and policymakers on potential options to improve borrower service, reduce defaults, develop best practices, assess consumer protections, and spur innovation.”

The CFPB estimates that there are more than 40 million borrowers with student loans who owe at least \$1.2 trillion –and 8 million borrowers are in default, owing more than \$110 billion. Problems with student loan servicers have been uncovered by the FDIC, other federal agencies and the CFPB itself. The request for information notes that the student loan servicing industry is not much different than the mortgage loan servicing industry, which has already come under strict scrutiny and rulemaking.

Federal Reserve Proposes Adding Munis to Bank Assets Needed for Liquidity

 The largest banks would be able to use certain general obligation state and municipal bonds to satisfy regulatory liquidity requirements under a new **Federal Reserve proposal**. The liquidity coverage ratio requirement mandates that large banks hold high-quality liquid assets that can be easily converted into cash within 30 days during a period of financial stress. The proposal would include investment-grade U.S. state and municipal bonds as high-quality liquid assets if they meet the criteria that apply to corporate debt securities.

OCC Eases Licensing Activities



After listening to banks complain about unnecessary requirements, the OCC has decided to integrate policies and procedures for corporate activities and transactions of national banks and savings associations. The **rule**

eliminates some requirements and makes technical changes that banks said were repetitive and unfair. The OCC said it is reviewing all its rules for savings associations and banks to see if it is possible to combine them to eliminate “unnecessary burden.”

FDIC Inspector General Says Better IT Exams Needed

The FDIC Inspector General says **better IT exams** are needed to combat cybersecurity threats. (See more about cybersecurity on p.2–3). The inspector general said third-party reviews are especially important since most audits seem to focus on internal controls over financial reporting rather than “security, availability, processing integrity, confidentiality, and privacy.” The inspector general also said that FDIC examiners should get better training on cyber risks.

TARP White Collar Prison Terms Hit 100

The office charged with investigating fraud surrounding the TARP program has **announced** that it has sent its 100th defendant to prison. The Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP) said so far 100 bankers, senior corporate executives, mortgage modification scammers, real estate developers, brokers, and others have been sentenced to prison time. SIGTARP said it is responsible for banning 93 individuals from various industries, including finance, banking, law and federal contracting. Its latest quarterly **report** to Congress noted that the most difficult cases to investigate were those involving bankers. SIGTARP said it had produced criminal charges against 29 bankers, but “we expect this number to rise significantly.” ■

About Invictus

*Invictus Consulting Group's bank analytics, strategic consulting, M&A and capital adequacy planning services are used by banks, regulators, investors and D&O insurers. For past issues of Bank Insights, please go to the **Invictus website**.*

*For editorial, email Lisa Getter at **lgetter@invictusgrp.com**. For information about Invictus, email **info@invictusgrp.com**.*