Banking
IN THE NINTH
SEPTEMBER 2016

NINTH DISTRICT HIGHLIGHTS

The Minneapolis Fed's Too Big to Fail Initiative: The Link to Community Banks


Ron Feldman

The Federal Reserve Bank of Minneapolis launched an initiative in 2016 to end the too big to fail (TBTF) problem (described here). Neel Kashkari, the Minneapolis Fed's president, argued that the problem was not solved as of 2016. And while he noted and supported the efforts under way to address TBTF, he also concluded that these efforts ultimately would not fix the problem. The initiative rests on the idea that now is the time to consider alternative, more transformative solutions.

Virtually all banks in the Ninth District are community banks. I know that people working at, providing services to and owning these banks follow banking-related news very closely. But they could fairly ask, "Does an effort aimed at the very largest banks matter to me?" In this column, I explain why the answer to this question is yes. In particular, efforts to right-size the regulation and supervision of community banks ultimately depend on reducing the chance of large bank bailouts. I expand on this conclusion after providing a little more detail on the Ending TBTF initiative.

The Minneapolis Fed's Ending TBTF Effort

The effort starts with concern over the current approach to addressing TBTF. A key component of the current approach is the idea that the government will stick losses on bondholders of large banks during a period of economic and financial stress. Making bondholders absorb the losses from bank failure will, under this plan, eliminate the need for the government to bail out the bank. Kashkari has noted that making bondholders take losses is at odds with what occurred during the most recent financial crisis and during the vast majority of such crises that have occurred in recent history. His view is informed by his direct involvement with the bailout decisions during the last crisis.

So a look at alternative approaches is needed. The Minneapolis Fed is considering a wide range of options, from "break up the bank" proposals to requiring the largest banks to hold much more capital than they do today. A key feature of the effort is engaging the public in considering how to address TBTF. Input directly from the public is requested here. The Reserve Bank has also hosted a series of meetings with experts around the country on options to address TBTF, which have been summarized and can be watched here. Kashkari will release a proposal to address TBTF by year-end 2016.

How Ending TBTF Links to Community Banks

Community banks focus on the families and firms in their areas.

continued on page 3

SAFETY & SOUNDNESS UPDATE

A Simple Exercise to Gauge Agricultural Banks' Susceptibility to Stress

Credit losses at agriculturally concentrated banks continue to be a top concern for the Ninth District. Commodity prices remain depressed despite recent gains, and nationwide average farm income is half of what it was two years ago. As a result, agricultural land values are declining throughout the Midwest, and nonperformance rates on loans have begun increasing at agriculturally concentrated banks.

In the September 2015 issue of *Banking in the Ninth*, Ron Feldman described work done with Joseph Smith in Minneapolis to understand the risk that falling agricultural land values would pose for agriculturally concentrated banks. We have done some simple follow-up work investigating how agricultural banks fare individually when hypothetically faced with loan loss rates from the farm crisis of the early 1980s. In this note, we describe how our initial findings

continued on page 2

for Ninth District banks suggest that many banks would suffer large capital declines when tested against extreme credit losses. That said, a large majority of agricultural banks would not fail despite the very extreme losses we impose on them in the exercise.

Key features of the agricultural bank exercise

Our analytical exercise is very simple and, in some sense, implausible. We assume banks with relatively large volumes of agricultural loans will face losses akin to some of the worst seen during the farm crisis of the early 1980s. We make a few assumptions about income and payouts and then determine the level of capital these banks would have after the stress scenario.

The stress scenarios we engineer do not represent our expectation about future losses and capital impacts at Ninth District banks; for all of these institutions to experience such severe loan losses simultaneously would be almost impossible. What, then, is the point? Picking an extreme scenario helps identify the individual banks that are susceptible to "tail" stress in the agricultural sector. It also sets out one extreme end of the potential results of a very stressful event for agricultural banks.

For the stress scenarios, we pick levels of loan loss based on those seen at the height of the farm crisis period (1984-87). We choose loss rates for agricultural loans and all other loans independently. They are mapped to banks based on the state in which they are headquartered. For instance, Nebraska's historical loss rates would be applied to a bank headquartered in Omaha. The loss rates are then applied to the current loan balances of banks.

We also make choices about other factors that would affect bank capital after accounting for loan losses. For instance, we might specify a suspension of dividend payments and equity buybacks, or set these values at the previous year's levels.

Stress scenarios

For our initial analysis, we subject our Ninth District banks to two scenarios:

- **Severe scenario**
  - 75th percentile agricultural loan loss rates from farm crisis period (state-by-state)
  - 75th percentile losses on other loans from farm crisis period (state-by-state)
  - Payouts (e.g., dividends and equity buybacks) are halted
- **Extremely severe scenario**
  - 95th percentile agricultural loan loss rates from farm crisis period (state-by-state)
  - 95th percentile losses on other loans from farm crisis period (state-by-state)
  - Payouts continue at the same level as in 2015

To be clear about what the severe scenario implies, the 95th percentile loss rate is the loss rate that only 5 percent of banks in that particular state faced or exceeded during the farm crisis. This means 95 percent of banks in that state had a lower loss rate. As noted, this scenario reflects a very extreme case: We are stressing all agricultural banks in a state against losses that only 5 percent of banks faced in the farm crisis.

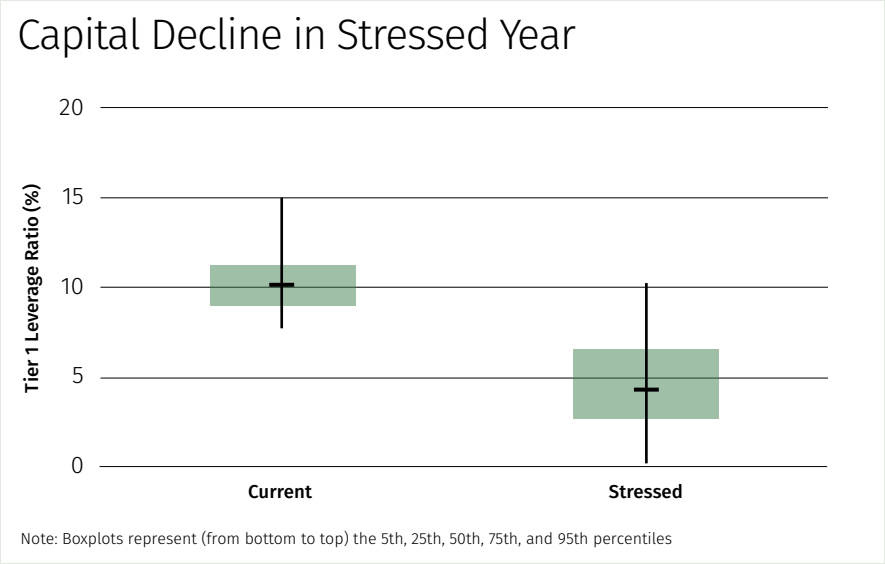
Initial findings for the Ninth District

We apply the loan loss rate and capital calculation choices to bank regulatory reporting data from the fourth quarter of 2015. We then examine the resulting changes in the tier 1 leverage ratio (tier 1 capital to average total capital).

End-state capital ratios reflect the severity of the scenario. After loan loss stress is applied, the average tier 1 leverage ratio drops from 10.6 percent to 10.1 percent in the mild scenario and to 5.0 percent in the severe scenario. In the severe scenario, approximately 45 percent of Ninth District banks' tier 1 leverage ratios drop below 4 percent, which is the Federal Reserve's current adequate capitalization threshold for this metric. Thus, we would classify 45 percent of these banks as being susceptible to crossing this regulatory threshold under very severe circumstances. The figure above shows the dramatic capital decline in the severe scenario across all the banks being examined. The figure is called a "box and whiskers" plot. The middle of the box shows the capital level for the "middle" or 50th percentile bank. The top of the box shows the 75th percentile, while the bottom of the box shows the 25th percentile. The top and bottom of the line shows the 95th and 5th percentile, respectively. In short, the current tier 1 leverage ratio (left) is much higher and less dispersed than the post-stress tier 1 leverage ratio (right).

This analysis has a number of limitations. It relies on data from the farm crisis, which may not reflect how stress in the agricultural sector would present itself today. It makes a number of simplifying assumptions about bank operations and performance. Finally, it does not take into account multiyear stressed scenarios.

Despite these limitations, it is a simple and transparent test that can identify banks that are susceptible to a worst-case scenario in the agricultural sector. Indeed, choosing an extreme case shows how large the losses have been in the past. That said, the graph suggests that a substantial majority of banks would survive this extreme test with positive capital, and likely would be able to continue supporting their community.



Note: Boxplots represent (from bottom to top) the 5th, 25th, 50th, 75th, and 95th percentiles

Strategies for Banks to Avoid Common Fair Credit Reporting Act Violations

By Liane M. Safar, Supervisory Examiner

The Fair Credit Reporting Act (FCRA) and Regulation V cover the rights of consumers related to their credit reports, including the obligations of credit reporting agencies (CRA) and the businesses that provide information to them. Examiners commonly identify violations related to these rules, given the number of technical requirements and the multiple business lines often covered by the requirements. In this article, we will summarize some of the most common violations we find. We then list steps that banks can take in advance to avoid such violations.

Common violations

Common violations include the following:

- Written Policies and Procedures[1]—Banks that provide customer credit information to CRAs must have written policies and procedures in place regarding the accuracy and integrity of that information. The regulation contains guidelines for what these policies and procedures should contain. Examiners often note that banks have accuracy and integrity policies, but they are often informal and not written. In addition, banks sometimes assume that other written policies, such as those related to identity theft red flags, cover the accuracy and integrity requirements, which is not usually the case.

- Risk-Based Pricing—Exception Notices[2] —Some banks use consumer reports to provide certain consumers with materially less favorable terms (e.g., higher rates or fees) than other consumers. When banks risk-base price in this manner, Regulation V requires that the consumer receive a risk-based pricing notice or a risk-based pricing exception notice (also known as a credit score notice). The exception notice is more common and contains a number of disclosures, including information about how banks use credit reports, score distributions, information about how the consumer's score compares to others, and information about the consumer's legal rights. Examiners commonly find errors related to these notices, such as missing content, failing to give a copy to each applicant, failing to provide the Notice to Home Loan Applicant on home equity lines of credit, and failing to provide a notice to consumers with no credit score.

- Adverse Action Notices[3] —A bank must provide an adverse action notice to the consumer when taking adverse action that is based on any information in a consumer report.[4] The notice must contain information such as the name of the CRA that provided the report, the consumer's right to receive a free report and dispute information, and credit score information, as applicable. The FCRA definition of "consumer report" is broad enough to cover more than just credit bureau reports. Examiners sometimes find that banks do not provide the required adverse action notice when the bank denies opening a deposit account because of information included in a consumer report (e.g., ChexSystems).

- Credit Reports for Employment Purposes[5]—Disclosure Format —A bank must give a written notice to the applicant informing the individual that a credit report will be obtained in order to receive authorization to pull a credit report as part of an employment application. The notice must be on a document that consists *solely* of the disclosure. Examiners commonly see the disclosure combined with other disclosures or documents, including as part of the actual employment application form.

What you can do

A few straightforward steps can help limit the potential for FCRA and/or Regulation V violations. First, compliance staff should familiarize themselves with the Federal Reserve's *Consumer Compliance Handbook*, which contains detailed summaries and examination procedures for most FCRA and Regulation V requirements.[6] The handbook has different modules that can be used to help focus compliance reviews or audits. Compliance staff can also use the procedures to learn about regulatory requirements and evaluate internal procedures for possible compliance weaknesses in this area.

Second, identify all of the business lines that use consumer reports and confirm how they use the reports. For example, employees who pull consumer reports when opening deposit accounts or hiring staff should be familiar with the FCRA adverse action requirements. These business lines

continued on page 4

NINTH DISTRICT HIGHLIGHTS *continued from page 1*

Senior managers at many such banks have told me that the post–financial crisis regulatory and supervisory regime is making this focus harder to maintain. Too much time is spent, they report, on compliance efforts that do not always create sufficient benefits for the community to justify the costs.

Policymakers at the Federal Reserve have taken some steps to address this concern. Most recently, Federal Reserve policymakers have suggested that the capital regime for small banks could be simplified. Efforts are also under way to reduce the reporting burden on small banks. I believe that many policymakers are open to further efforts to right-size the regulation and supervision that community banks face.

But concern about the TBTF status of the largest banks is a potential roadblock to improving regulation and supervision of smaller banks. Why? My sense is that some policymakers and elected officials worry about any significant relaxation of supervision and regulation in a period when TBTF remains a problem. They might worry that efforts to address community bank concerns would get linked to efforts to roll back supervision and regulation of the largest entities. Or perhaps the idea of any major change in post–financial crisis supervision and regulation seems premature when the job is not yet completed for the largest banks. Also, the public may not want much change until they are confident that bailouts cannot readily occur again.

There is no guarantee, of course, that completing efforts to end TBTF will lead to more risk-focused supervision and regulation of community banks. But the odds of providing regulatory relief for small banks seem better when concerns about the largest banks have been addressed. This suggests a strong link between the Minneapolis Fed's Ending TBTF effort and an issue of central importance to community banks.

Managing the Increasing Risk of Ransomware

By Rory Guenther CISA, Senior Examiner

On November 3, 2015, the FFIEC issued a statement alerting financial institutions to an increase in both severity and frequency of cyber attacks, often involving the use of ransomware. Cybercriminals have been using ransomware for several years but have recently shifted their focus to financial institutions, and we have had reports of ransomware incidents in the Ninth District. I will provide a basic overview of ransomware and the potential implications of a ransomware event. I will also highlight some nontechnical actions from the FFIEC statement that can specifically help manage risks related to ransomware.

What is ransomware?

Ransomware is a type of malware that typically encrypts data on a target machine and/or connected network. The program is often introduced when an employee opens an email attachment or clicks on a malicious web page or ad. Cybercriminals then extort the victim organization for payment in order to release or unlock the files. Attackers commonly request payment using the electronic currency Bitcoin, making it nearly impossible for law enforcement to track.

Potential impact of a ransomware event

Hackers have customized ransomware to not only infect and encrypt data on an individual machine, but also to spread across any connected network to other workstations, servers, backup devices, or connected third parties. If your organization becomes a victim, the implications could range from disconnecting and recovering a single workstation to having multiple servers, databases, and entire systems becoming unavailable. You may also be impacted by a ransomware incident at a critical service provider or third party.

Protecting your organization from ransomware

In the November press release, the FFIEC references existing risk management guidance and specifically highlights eight general steps financial institutions should consider. Management should review the press release and take into account all of these important actions to address overall cybersecurity risk management. For the remainder this article, I will focus on some nontechnical control activities management should take into consideration, which could significantly minimize both the chance of an incident and the impact it has on your organization.

Nontechnical ways to manage ransomware risks

Review and update information security awareness and training programs to include cyber attacks involving extortion and to foster a culture that encourages disclosure.

The most effective way to prevent a ransomware incident is to educate staff on the importance of cybersecurity, to prevent them from clicking on suspicious attachments, or visiting unnecessary websites. Getting employees to understand the potential implications for the entire organization is a critical milestone to managing this risk.

It is also important for management to foster an open corporate culture that encourages honest and prompt reporting when an incident may have occurred. Employees who believe they will be punished for even a one-time mistake might avoid reporting anything suspicious. This silence can lead to a much greater loss for the organization if ransomware has time to spread across the network.

Review, update, and periodically test incident response plans to minimize risk and disruption should a ransomware incident occur.

Financial institutions should have incident response plans that are up to date, realistic, and sufficiently tested. Regulators are increasingly looking for evidence of regular testing. Management should ask itself and staff the following questions to assist in this review: Does your current incident response plan adequately respond to a ransomware incident? Does your plan consider nontechnical decisions that you would need to make? Does the plan include reliance on third parties? Have you discussed the plan with service providers and included them in testing? Would their priorities or capabilities change if a ransomware incident was impacting multiple customers? Who should you notify in case of an incident?

Management should also include a ransomware incident as a scenario or a tabletop exercise as part of regular testing of your response plans. Involve nontechnical staff in the discussions to reinforce awareness. Questions to ask during that scenario could include: Would you pay the ransom? Or would it depend on the criticality of the data, the potential downtime, or the cost to recover from backup? How much is an hour of downtime worth?

An oft-cited sentiment in the information security industry is that *it is not **if** you get hacked, but **when** you get hacked.* Be sure your organization is prepared to respond and minimize the impact of a ransomware incident by educating employees and testing incident response plans.

CONSUMER AFFAIRS UPDATE *continued from page 3*

should have processes for ensuring that the bank complies with these requirements when appropriate. The bank's internal and/or external audit should periodically verify compliance with these requirements. Likewise, consumer lenders who originate loans secured by one-to-four family residential real estate (e.g., home equity lines of credit) should ensure that they understand how to generate compliant risk-based pricing exception notices for both consumer loans and dwelling-secured loans.

Finally, periodically check the content of risk-based pricing exception notices and adverse action forms, even if you are using forms from a vendor, such as a CRA. In addition, make sure all of the default settings are correct in your automated disclosure systems and review the disclosure content after any software updates. Many times, violations related to missing content occur because disclosure templates or default settings are incorrect.

---

[1] Regulation V section 1022.42
[2] Regulation V section 1022.74
[3] FCRA section 615(a)
[4] Regulation B—Equal Credit Opportunity Act has additional requirements that apply when a bank takes adverse action on a loan application.
[5] FCRA section 604(b)
[6] *Consumer Compliance Handbook*, http://www.federalreserve.gov/boarddocs/supmanual/supervision_cch.htm