Supervisory Insights

Devoted to Advancing the Practice of Bank Supervision

Vol. 12, Issue 2 Winter 2015

Inside

A Framework for Cybersecurity

Marketplace Lending

Lending Viewpoint: Results from the FDIC's Credit and Consumer Products/ Services Survey

Regulatory and Supervisory Roundup

FDIC

Supervisory Insights

Supervisory Insights is published by the Division of Risk Management Supervision of the Federal Deposit Insurance Corporation to promote sound principles and practices for bank supervision.

Martin J. Gruenberg
Chairman, FDIC

Doreen R. Eberley
Director, Division of Risk Management Supervision

Supervisory Insights is available on-line by visiting the FDIC's Web site at www.fdic.gov. To provide comments or suggestions for future articles, request permission to reprint individual articles, or request print copies, send an e-mail to SupervisoryJournal@fdic.gov.

Issue at a Glance

Volume 12, Issue 2 Winter 2015

Letter from the Director 2

Articles

A Framework for Cybersecurity 3

Due to the increase in number and sophistication of cyber threats, cybersecurity has become a critical issue facing the financial services sector. This article discusses the cyber threat landscape and how financial institutions' information security programs can be enhanced to address evolving cybersecurity risks. The article concludes with a discussion of actions taken by the federal banking agencies in response to the increase in cyber threats.

Marketplace Lending 12

Some banks are finding the small, but growing arena of marketplace lending to be an attractive source of revenue. This article provides an overview of the marketplace lending model and the associated risks, including those that arise in third-party arrangements. The article also highlights the importance of a pragmatic business strategy and offers resources for bank boards of directors and management teams to consider when engaging in marketplace lending activity.

Lending Viewpoint: Results from the FDIC's Credit and Consumer Products/Services Survey 19

Prudent loan risk selection and close monitoring of the lending portfolio remain critical components of a well-managed bank. Therefore, FDIC examiners continue to carefully assess lending and the related risks during the post-crisis rebound in lending. This article describes recent lending conditions and risks as reported through the Credit and Consumer Products/Services Survey.

Regular Features

Regulatory and Supervisory Roundup 27

This feature provides an overview of recently released regulations and supervisory guidance.

Letter from the Director

The banking industry continues to face challenges in traditional business lines, new product offerings, and from cyber attacks on information security systems. The articles in this issue of *Supervisory Insights* provide information and resources for bankers and examiners in three areas — the evolving arena of cybersecurity, marketplace lending, and current lending portfolio conditions and risks.

Due to the growing sophistication and number of cyber attacks, cyber security has become a critical issue facing the financial services sector. "A Framework for Cybersecurity" provides an overview of the current cyber threat landscape, and discusses how banks can enhance and leverage existing security and governance practices into effective information security programs. The article concludes with a review of actions the federal banking agencies have taken in response to cyber threats.

Marketplace lending is a small but growing component of the financial services industry that some banks are viewing as an opportunity to increase revenue. "Marketplace Lending" describes the marketplace lending model and highlights the risks banks may face in dealing with marketplace lenders, particularly when those associations are in the form of third-party arrangements. The article identifies resources for bank management and directors to consider when participating in marketplace lending activity.

Careful monitoring of the loan portfolio and identification of potential risks remain characteristics of a well-managed bank. "Lending Viewpoint: Results from the FDIC's Credit/Consumer Products and Services Survey" provides an overview of current lending conditions as reported by this survey following FDIC risk management examinations. Data from the survey continue to help the FDIC assess lending trends at the banks we supervise and proactively address any areas of heightened risk.

This issue of *Supervisory Insights* also includes an overview of recently released regulatory and supervisory guidance.

I hope you find the articles in this issue to be informative and useful. We encourage our readers to provide feedback and suggest topics for future issues. Please e-mail your comments and suggestions to SupervisoryJournal@fdic.gov.

Doreen R. Eberley
Director
Division of Risk Management Supervision

A Framework for Cybersecurity

During the past decade, cybersecurity has become one of the most critical challenges facing the financial services sector due to the frequency and increasing sophistication of cyber attacks. In response, financial institutions and their service providers are continually challenged to assess and strengthen information security programs and refocus efforts and resources to address cybersecurity risks.

This article describes the evolving cyber threat landscape and the U.S. government's response to enhance the security and resilience of the nation's critical infrastructure sectors. The article discusses how components of financial institutions' information security programs, including corporate governance, security awareness training, and patch-management programs, should be enhanced to address cybersecurity risks, and concludes with an overview of actions taken by the federal banking agencies to respond to cyber threats.

The Evolving Threat Landscape

Historically, a bank's primary security concern centered on protecting physical data assets such as posted ledger cards, promissory notes, and critical documents in the vault as well as securing the perimeter of the bank premises. In today's banking environment, business functions and technologies are increasingly interconnected, requiring financial institutions to secure a greater number of access points. Innovation has resulted in greater use of automated core processing, document imaging, distributed computing, automated teller machines, networking technologies, electronic payments, online banking, mobile banking, and other emerging technologies. At the same time, physical data assets have been automated and a bank's sensitive customer information stored on computers has become as valuable as currency—a different kind of asset that needs safeguarding.

Cyber criminals use a variety of tactics. Some more common attack strategies in recent years include malicious software deployment, distributed denial-of-service (DDoS) attacks, and compound attacks.

Malware

Malicious software, commonly referred to as "malware," is a broad class of software generally used to gain access to or to damage a computer or system. Malware may infect a computer from a variety of access points. Perpetrators often include malware as an attachment to an email, or it is delivered from websites referenced in emails. The perpetrator tricks the email recipient into reading the email and opening the attachment or clicking on the link by crafting the email to look as though it came from a trusted source.

These emails that deliver the malware are often referred to as "phishing" emails as they are fishing for victims. A "spear phishing" email campaign is a subset of phishing in which the email content is tailored to the interests of a smaller group or a single recipient. Phishing and spear phishing campaigns mislead targets into providing sensitive information such as user names, passwords, credit card details, or personal sensitive information, such as date of birth and Social Security number, that can be used to commit identity theft against the individual or gain access to

A Framework for Cybersecurity

continued from pg. 3

bank systems for theft, disruption, or destruction.

Examples of malware include ransomware and wiper programs. "Ransomware" generally restricts all access to a computer and demands a ransom be paid for access to be restored. "Wiper" programs destroy data from the infected computer's hard drive and, in some cases, may be used to cover the attacker's tracks.

Distributed Denial-of-Service

A DDoS attack attempts to make a machine or network connected to the Internet unavailable to its intended users by overloading it with excessive Internet traffic. Given the nature of these attacks, DDoS attacks cannot be prevented, but they can be successfully mitigated. The ability to effectively manage a DDoS attack comes from the target's ability to control and recover from the attack, possibly by redirecting Internet traffic to a different server or engaging a DDoS mitigation service.

Compound Attacks

Another attack strategy is the use of "compound attacks," in which more than one method of attack is deployed simultaneously. For example, criminals have used DDoS attacks to distract a target organization while perpetrating another form of attack. Or a phishing email may contain an attachment or link that, if clicked by the target, downloads a seemingly harmless file that contains hidden malicious software with delayed execution commands.

As the banking industry necessarily innovates to take advantage of new technologies and delivery channels, it needs to be alert to any related new avenues of cyber attacks. Banks can help mitigate these attacks by developing an effective cybersecurity awareness campaign for employees and customers, a comprehensive patching program, and a strong detection program. A sound risk-management program and corresponding controls will help mitigate the threat of cyber attacks.

A Critical Infrastructure Perspective

On February 12, 2013, the President issued Executive Order 13636, "*Improving Critical Infrastructure Cybersecurity*," which established that "[i]t is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." The Executive Order directed the National Institute of Standards and Technology (NIST) to develop a risk-based cybersecurity framework to serve as a set of voluntary consensus standards and industry best practices to help organizations manage cybersecurity risks. The NIST[1] defines cybersecurity as "the process of protecting information by preventing, detecting, and responding to attacks."

The NIST *Framework for Improving Critical Infrastructure Cybersecurity*[2] was created through collaboration

[1] NIST is a non-regulatory, federal agency within the U.S. Department of Commerce. See: www.nist.gov.

[2] The Framework for Improving Critical Infrastructure Cybersecurity can be found at: http://www.nist.gov/cyberframework/.

between industry and government and consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The first version of the cybersecurity framework was released on February 12, 2014, and consisted of five core areas: Identify, Protect, Detect, Respond, and Recover.

The cybersecurity definition and the components in the framework are similar to the concepts found in Appendix B to Part 364 of the FDIC's Rules and Regulations. Appendix B was established as a result of the enactment of the *Gramm-Leach-Bliley Act* in 1999 and required each financial institution to develop an information security program. Use of the cybersecurity framework is not intended to replace a bank's traditional information security program, but rather modify the program to address emerging cyber risks. A bank's information security program should evolve as the operating environment and the threat landscape change. An effective information security program is not static and should be regularly evaluated and updated.

Bank management must incorporate cybersecurity into the bank's overall risk-management framework; design and implement appropriate mitigating controls; update respective policies and procedures and, ultimately, validate the intended control structure through an audit program. When designing a cyber risk control structure, four components of traditional information security programs are critical: Corporate Governance, Threat Intelligence, Security Awareness Training, and Patch-Management Programs.

Corporate Governance of Cybersecurity

An institution's executive management and Board of Directors (board) play a key role in overseeing programs to protect data and technology assets and establishing a corporate culture consistent with the bank's risk tolerance. A bank should evaluate and manage cyber risk as it does any other business risk. It is not simply the obligation of those employees in the server room, but rather an enterprise-wide initiative involving all employees. It is critical the board institute a corporate culture prioritizing cybersecurity.

Threat Intelligence

The Federal Financial Institutions Examination Council (FFIEC) on November 3, 2014, issued "*Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement*." The statement indicates that, "[f]inancial institution management is expected to monitor and maintain sufficient awareness of cybersecurity threats and vulnerability information so they may evaluate risk and respond accordingly." Essentially, it states that each financial institution should have a program for gathering, analyzing, understanding, and sharing information about vulnerabilities and threats to arrive at "actionable intelligence." Actionable intelligence can be gathered from various public and private sources.

The FFIEC statement encouraged financial institutions to participate in the Financial Services Information Sharing and Analysis Center (FS-ISAC)[3] as a source of threat intelligence.

[3] The FS-ISAC is a non-profit, information-sharing forum established by financial services industry participants to facilitate the public and private sectors' sharing of physical and cybersecurity threat and vulnerability information. See: www.fsisac.com.

A Framework for Cybersecurity

continued from pg. 5

FS-ISAC is a public-private partnership that operates as an information-sharing forum. It was established by a Presidential directive to facilitate the sharing of threat and vulnerability information among critical infrastructure sectors. FS-ISAC information includes analysis and mitigation strategies about a multitude of topics including, but not limited to, information security, physical security, business continuity and disaster recovery, fraud investigations, and payment system risk. FS-ISAC also provides additional services and membership benefits including participation in webinars, workshops, threat exercises, and assistance in creating information filters to ensure an institution is receiving the threat and intelligence information it needs without experiencing information overload. To obtain this assistance, an institution need only call FS-ISAC toll-free at (800) 464-0085. In addition, FS-ISAC has created a community bank working group and sends weekly cyber updates to community bank executives. These updates use layman's language to explain the most pertinent cyber events of the week and to provide strategies for making the information actionable.

Another source of cyber intelligence is the U.S. Computer Emergency Readiness Team (US-CERT). US-CERT is part of the Department of Homeland Security and is focused on information regarding current security issues, vulnerabilities, and exploits. In addition to alerts, which an institution can receive by subscribing at www.us-cert.gov, US-CERT offers publications, educational material, and some assistance with cyber threats.

Security Awareness Training

Even the best-designed security controls cannot fully protect a financial institution from one uninformed employee, contractor, or customer who unwittingly visits a malicious Web site, opens a malicious email attachment, or clicks on a malicious email link. Effective cybersecurity awareness programs should educate employees, contractors, and customers about the threat environment and encourage them to "*Think Before You Click*."

Cybersecurity awareness programs should highlight the importance of guarding against cyber risks across all business lines and functions. Employees from entry-level staff to the board should participate in mandatory cybersecurity awareness training, as one uninformed employee can be the bank's weakest link.

Security awareness training should be role-specific, as job functions require access to different systems and types of information with varying levels of sensitivity. Cyber attacks may be customized and targeted at employees with greater access to data or the ability to modify security settings or install new applications, or those with the ability to initiate or authorize the transfer of funds. For example, frequent targets include information security professionals, executives, comptrollers, and cashiers.

Cybersecurity awareness training should be available to bank personnel and contractors as well as bank customers, merchants, and other third parties, as they represent additional access points to a bank's data systems

and can be targets of cyber criminals. For example, corporate account takeovers are typically perpetrated by the theft of a customer's login credentials that are used to transfer money from compromised accounts.

Patch-Management Programs

The lack of an effective patch-management program has contributed significantly to the increase in the number of security incidents. Patches are software updates designed to fix known vulnerabilities or security weaknesses in applications and operating systems.

An effective patch-management program should include written policies and procedures to identify, prioritize, test, and apply patches in a timely manner. The first step is to create an asset inventory cataloging the systems requiring patch-management oversight. The asset inventory should capture all software and firmware, such as routers and firewall operating systems, which are subject to periodic patches from vendors.

An effective program also should use information received from threat intelligence sources that report on identified vulnerabilities. Bank management should be aware of products reaching or at the end-of-life or those no longer supported by a vendor. Management should also establish strategies to migrate from unsupported or obsolete systems and applications and, in the interim, implement strategies to mitigate any risk associated with the use of unsupported or obsolete products.

The board and senior management should require regular, standard reporting (metrics) on the status of the patch-management program, including reports that monitor the identification and installation of available patches. Independent audits and internal reviews should validate the effectiveness of patch-management programs.

Regulatory Response and Resources

The FDIC monitors cybersecurity issues on a regular basis through on-site bank examinations, regulatory reports, and intelligence reports. The Corporation continually evaluates its own supervisory policies for potential improvement and encourages practices to protect against threats at the banks it supervises. The FDIC has taken a number of steps to increase industry awareness of cyber risks and to provide practical tools to help mitigate the risk of cyber attack.

In the spring of 2014, the FDIC issued a press release urging institutions to actively utilize available resources to identify and help mitigate potential cyber-related risks. It is important for financial institutions of all sizes to be aware of the constantly emerging cyber threats and government-sponsored resources available to help identify these threats on a real-time basis. The press release contained a number of examples of free resources available to institutions and their website addresses.

In the summer of 2014, the FDIC developed and issued the "Cyber Challenge" exercise, a resource for community banks to use in assessing their preparedness for a cyber-related incident, through a series of videos and simulation exercises that depicted actual events experienced by institu-

A Framework for Cybersecurity

continued from pg. 7

tions. The Cyber Challenge exercise is available free to all institutions on the FDIC website, www.fdic.gov, under the Community Banking Initiative link.[4]

In the summer of 2015, the FDIC created a cybersecurity awareness training program for FDIC-supervised institutions, as well as FDIC supervision staff and management. These sessions were held in each of the FDIC's regional offices during August 2015. One banker stated that during his examination after the session, he found great benefit in discussing what both he and his examiner heard at the cyber awareness training the week before. The training program was followed by a teleconference in October 2015 to provide an overview of the program and to share commonly asked questions and answers.

Lastly, in November 2015, the FDIC added three additional video simulation exercises to Cyber Challenge as well as a Cybersecurity Awareness video that provides an overview of the threat environment and steps community financial institutions can take to be better prepared should a cyber-attack occur. These materials are available free on the FDIC website, www.fdic.gov, under the Community Banking Initiative link.

The FDIC has also participated in a number of other activities as a member of the Federal Financial Institutions Examination Committee or FFIEC. In June 2013, the FFIEC created the Cybersecurity and Critical Infrastructure Working Group (CCIWG). The CCIWG's first major undertaking was to work to determine how well banks, particularly community banks, manage cybersecurity and to assess banks' preparedness to mitigate cyber risks. The FFIEC members conducted a pilot cybersecurity assessment during 2014 at more than 500 community institutions to evaluate preparedness. The results were reflected in the FFIEC document, "*Cybersecurity Assessment General Observations*," which provided themes from the assessment and suggested questions for chief executive officers and boards of directors to consider when assessing institutions' cybersecurity preparedness.[5]

The CCIWG also reviewed all outstanding regulatory guidance to identify any gaps and, as a result, the FFIEC IT Examination Handbook and other relevant regulatory guidance are being updated to address cybersecurity concerns. The CCIWG publishes cybersecurity information at http://www.ffiec.gov/cybersecurity.htm. The chart below provides an overview of recently released supervisory guidance and other FDIC or FFIEC resources that bank management may find useful in addressing cybersecurity risks.

[4] https://www.fdic.gov/regulations/resources/director/technical/cyber/purpose.html.

[5] The "FFIEC Cybersecurity Assessment General Observations" presents general observations from the Cybersecurity Assessment about the range of inherent risks and the varied risk management practices among financial institutions. See: http://www.ffiec.gov/press/pr110314.htm.

Regulatory Action/Resource	Summary
Cybersecurity Awareness Technical Assistance Videos	This video series titled Cybersecurity Awareness is designed to assist bank directors with understanding cybersecurity risks and related risk management programs and to elevate cybersecurity discussions from the server room to the board room. The first video covers the evolution of data security, defines cybersecurity, and reviews the current cybersecurity threat environment. The second video reviews the components of traditional information security programs and discusses how elements of the program should be refocused in the current cybersecurity threat environment. See https://www.fdic.gov/regulations/resources/director/technical/cybersecurity.html
Vendor Management Technical Assistance Video	This video titled Outsourcing Technology Services is designed to assist bank directors with understanding responsibilities for governing their institution's vendor risk management program. The components of a program include a risk assessment process, service provider selection, contract negotiation and evaluation, and an ongoing monitoring framework. The video also discusses business continuity planning and testing and resources to assist with establishing and maintaining a vendor risk management program. To be released in early 2016.
Cyber Challenge: A Community Bank Cyber Exercise	The FDIC's simulation exercise, Cyber Challenge, is designed to encourage community financial institutions to discuss operational risk issues and the potential impact of information technology disruptions on common banking functions. Using seven unique scenarios, the Cyber Challenge helps start an important dialogue among bank management and staff about ways they address operational risk today and techniques they can use to mitigate this risk in the future. Cyber Challenge is not a regulatory requirement; it is a technical assistance tool designed to help assess operational readiness. See https://www.fdic.gov/regulations/resources/director/technical/cyber/purpose.html
Corporate Governance Technical Assistance Video	This presentation reviews corporate governance principles that are vital to a director's role in setting the direction of the bank. It focuses on three areas: (1) the role of a bank director, the associated responsibilities, and the importance of independent decision making; (2) direction on the supervision of bank operations; and (3) guidance to help directors stay informed. See https://www.fdic.gov/regulations/resources/director/virtual/governance.html
Information Technology (IT) Technical Assistance Video	The IT video is designed to enhance bank directors' awareness of effective risk management practices. The video illustrates key IT governance programs, discusses select emerging and significant IT risks, and provides relevant questions to consider at the directorate level. By doing so, it provides a reasonable foundation for bank directors to exercise their fiduciary oversight over ever-changing and challenging IT risks. See https://www.fdic.gov/regulations/resources/director/virtual/it.html

A Framework for Cybersecurity

continued from pg. 9

FFIEC Statement on Cyber Attacks Involving Extortion	This FFIEC statement, dated November 3, 2015, notified financial institutions of the increasing frequency and severity of cyber attacks involving extortion. It advised financial institutions to develop and implement effective programs to ensure the institutions are able to identify, protect, detect, respond to, and recover from these types of attacks. See http://www.ffiec.gov/press/PDF/FFIEC_Joint_Statement_Cyber_Attacks_Involving_Extortion_-_Interactive_Ve%20%20%20.pdf
FFIEC Cybersecurity Assessment Tool	On June 30, 2015, the FDIC, in coordination with the other FFIEC member agencies, issued the FFIEC Cybersecurity Assessment Tool to help institutions identify cybersecurity risks and determine their preparedness. Similar to a bank's information security program risk assessment, this voluntary tool provides management with a repeatable and measurable process to assess an institution's risks and cybersecurity preparedness. See http://www.ffiec.gov/cyberassessmenttool.htm
FFIEC Webinar: Executive Leadership of Cybersecurity: What Today's CEOs Need to Know About the Threats They Don't See	On May 7, 2014, the FFIEC's CCIWG hosted a Webinar entitled, Executive Leadership of Cybersecurity: What Today's CEOs Need to Know About the Threats They Don't See. The webinar was intended to raise awareness about the pervasiveness of cyber threats, discuss the role of executive leadership in managing these risks, and to share actions being taken by the FFIEC. See https://www.youtube.com/watch?v=t1ZgWKjynXI&feature=youtu.be
FFIEC Statement on Destructive Malware	This FFIEC statement, dated March 30, 2015, notified financial institutions of the increasing threat of cyber attacks involving destructive malware. It warned that financial institutions and technology service providers should enhance information security programs to ensure they are able to identify, mitigate, and respond to this type of attack. In addition, the statement recommended that business continuity planning and testing activities incorporate response and recovery capabilities and test resilience against cyber attacks involving destructive malware. See http://www.ffiec.gov/press/PDF/2121759_FINAL_FFIEC%20Malware.pdf
FFIEC Statement on Cyber Attacks Compromising Credentials	This FFIEC statement, dated March 30, 2015, notified financial institutions of the growing trend of cyber attacks for the purpose of obtaining online credentials for theft, fraud, or business disruption and to recommend risk mitigation techniques. It said financial institutions should address this threat by reviewing their risk management practices and controls over information technology (IT) networks and authentication, authorization, fraud detection, and response management systems and processes. See http://www.ffiec.gov/press/PDF/2121758_FINAL_FFIEC%20Credentials.pdf
Appendix J to the Business Continuity Planning IT Booklet: Strengthening the Resilience of Outsourced Technology Services	On February 6, 2015, the FFIEC issued an update (Appendix J) to the Business Continuity Planning IT Booklet entitled "Strengthening the Resilience of Outsourced Technology Services." This update stresses the importance of addressing and incorporating cybersecurity elements when establishing and monitoring third-party relationships. See http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-j-strengthening-the-resilience-of-outsourced-technology-services.aspx

FFIEC Statement on Cybersecurity Threat and Vulnerability Monitoring and Sharing	This statement, dated November 3, 2014, indicated that financial institution management is expected to monitor and maintain sufficient awareness of cybersecurity threats and vulnerability information so they may evaluate risk and respond accordingly. It stated that each financial institution should have programs for gathering cyber-related information about vulnerabilities and threats in a timely manner, analyzing the data, and sharing information to arrive at "actionable intelligence." The statement also encouraged financial institutions to participate in the FS-ISAC as a source of threat intelligence. FS-ISAC information includes analysis and solutions about a multitude of topics including, but not limited to, information security, physical security, business continuity and disaster recovery, fraud investigations, and payment system risk. See http://www.ffiec.gov/press/pr110314.htm

Conclusion

Cyber risk is a substantial business risk. A bank's board and senior management must understand the seriousness of the threat environment and create a cybersecurity culture throughout the organization. The effective identification and mitigation of cyber risk must be grounded in a strong governance structure with the full support of the board and senior management.

Michael B. Benardo
Chief, Cyber Fraud and Financial Crimes Section
Division of Risk Management Supervision
mbenardo@fdic.gov

Kathryn M. Weatherby
Examination Specialist (Fraud)
Cyber Fraud and Financial Crimes Section
Division of Risk Management Supervision
kweatherby@fdic.gov

Marketplace Lending

Marketplace lending is a small but growing alternative to traditional financial services for consumers and small businesses. Attracted by opportunities for earnings growth, some banks have entered the marketplace lending business either as investors or through third-party arrangements. As with any new and emerging line of business, marketplace lending can present risks. Financial institutions can manage these risks through proper risk identification, appropriate risk-management practices, and effective oversight. Conversely, failure to understand and manage these risks may expose a financial institution to financial loss, regulatory action, and litigation, and may even compromise an institution's ability to service new or existing customer relationships. Before participating in marketplace lending, financial institution management should identify potential vulnerabilities and implement an effective risk-management strategy that protects the bank from undue risk.

This article is intended to heighten bankers' and examiners' understanding of marketplace lending and potential associated risks, including those arising in third-party arrangements. The article also highlights the importance of a pragmatic business strategy that considers the degree of risk together with the potential revenue stream, and emphasizes the importance of banks exercising the same due diligence they practice whenever they extend credit to a borrower.

Marketplace Lending Defined

For purposes of this article, marketplace lending is broadly defined to include any practice of pairing borrowers and lenders through the use of an online platform without a traditional bank intermediary. Although the model, originally started as a "peer-to-peer" concept for individuals to lend to one another, the market has evolved as more institutional investors have become interested in funding the activity. As such, the term "peer-to-peer lending" has become less descriptive of the business model and current references to the activity generally use the term "marketplace lending."

Marketplace lending typically involves a prospective borrower submitting a loan application online where it is assessed, graded, and assigned an interest rate using the marketplace lending company's proprietary credit scoring tool. Credit grades are assigned based on the marketplace lending company's unique scoring algorithm, which often gives consideration to a borrower's credit score, debt-to-income ratio, income, and other factors set by the marketplace lender. Once the application process is complete, the loan request is advertised for retail investors to review and pledge funds based on their investment criteria. A loan will fund from the monies collected if investors pledge sufficient capital before the deadline stated in the loan request (*e.g.* 14 days after the request is posted). As an alternative to funding loans through such retail investments, institutional investors can provide funding through whole loan purchases or direct securitizations.

When a borrower's requested loan amount is fully pledged, the market-

Figure 1: Illustration of Direct Funding Model

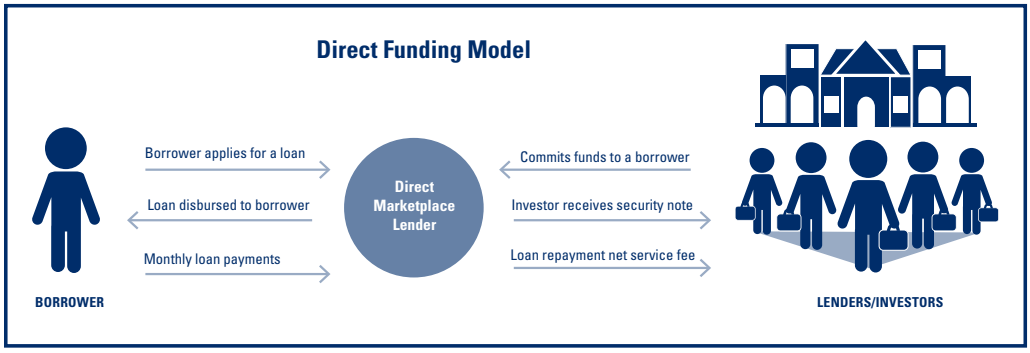
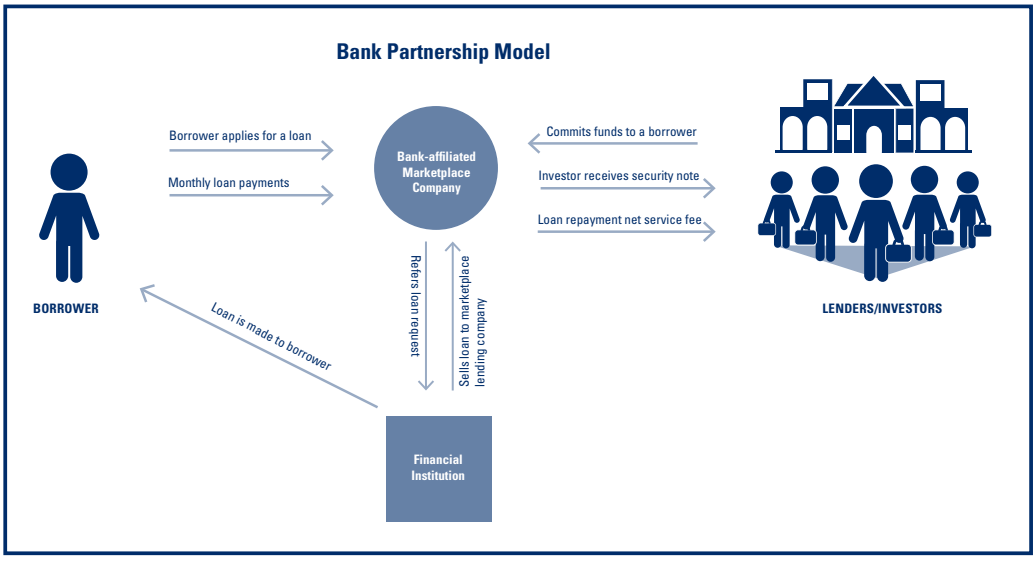


Figure 2: Illustration of Bank Partnership Model



place lending company originates and funds the loan through one of two frameworks: 1) the company lends the funds directly (subsequently referred to as a " direct marketplace lender") or 2) the company partners with a traditional bank to facilitate the loan transaction (subsequently referred to as a "bank-affiliated marketplace company").

A direct marketplace lender typically is required to be registered and licensed to lend in the respective state(s) in which it conducts business. Direct marketplace lenders facilitate all elements of the transaction, including collecting borrower applications, assigning credit ratings, advertising the loan request, pairing borrowers with interested investors, originating the loan, and servicing any collected loan payments. As part of the transaction, direct marketplace lenders issue investors either registered or unregistered security notes (subsequently referred to as "security notes") in exchange for the investments used to fund the

Marketplace Lending

continued from pg. 13

loan. Consequently, the borrower's repayment obligation remains with the direct marketplace lender, the security notes issued to investors become the obligation of the direct marketplace lender, and the investors are unsecured creditors of the direct marketplace lender. (See Figure 1 on the previous page for an illustration of this process.)

Some marketplace lending companies operate under the second framework by working through a cooperative arrangement with a partner bank. In these cases, the bank-affiliated marketplace company collects borrower applications, assigns the credit grade, and solicits investor interest. However, from that point the bank-affiliated marketplace company refers the completed loan application packages to the partner bank that makes the loan to the borrower. The partner bank typically holds the loan on its books for 2-3 days before selling it to the bank-affiliated marketplace company. Once the bank-affiliated marketplace company purchases the loan from the partner bank, it issues security notes up to the purchase amount to its retail investors who pledged to fund the loan. By the end of the sequence of transactions, the borrower's repayment obligation transfers to the bank-affiliated marketplace company, and the security noteholder maintains an unsecured creditor status to the bank-affiliated marketplace company, which mirrors the outcomes described under the direct funding framework (see Figure 2 on the previous page). In certain circumstances, some institutional investors may invest in whole loan transactions, which are often arranged directly between the interested parties and outside any cooperative arrangement with a partner bank.

Once the process is complete, borrowers begin making fixed monthly payments to the bank-affiliated marketplace company which issues a pro rata payment to the investor, less loan servicing fees.

Common barriers to entry for banks and other traditional financial services entities include state licensure laws, capital requirements, access to financing, regulatory compliance, and security concerns. Some of these barriers may not exist for marketplace lending companies. New start-up marketplace lenders may be established quickly and often with a unique niche to capture a particular share of the market. In 2009, industry analysts with IBISWorld identified at least three marketplace lending companies; by 2014, the number had grown to 63 marketplace lending companies.[1] As of September 2015, the number of established marketplace lending companies totaled 163 with new entrants continuing to join the competitive market.[2]

Concomitant with the increasing number of market participants, new or expanded product lines are introduced as companies attempt to establish a niche position in the market. Some examples of marketplace loan products include unsecured

[1] Omar Khedr, "Front money: Revenue will rise, but regulations threaten industry profitability," IBISWorld Industry Report OD4736 Peer-to-Peer Lending Platforms in the US, December 2014. (A subscription to IBISWorld is needed to view this report.) http://clients1.ibisworld.com/reports/us/specializedreportsarchive/default.aspx?entid=4736.

[2] Omar Khedr, "Street credit: New industry's explosive growth may meet regulatory hurdles," IBISWorld Industry Report OD4736 Peer-to-Peer Lending Platforms in the US, September 2015. (A subscription to IBISWorld is needed to view this report.) http://clients1.ibisworld.com/reports/us/industry/default.aspx?entid=4736.

consumer loans, debt consolidation loans, auto loans, purchase financing, education financing, real estate lending, merchant cash advance, medical patient financing, and small business loans.

The Importance of Effective Risk Identification

The marketplace lending business model depends largely on the willingness of investors to take on the credit risk of an unsecured consumer, small business owner, or other borrower. Given the market's infancy and that it has primarily existed in an environment of low and steady interest rates, current credit loss reports or loss-adjusted rates of return may not provide an accurate picture of the risks associated with each marketplace lending product.

Further, each marketplace lending company's risk level and composition varies depending on the business model or credit offering, with potentially significant variations across credit products. Given the credit model variations that exist, using a nonspecific approach to risk identification could lead to an incomplete risk analysis in the bank's marketplace investments or critical gaps in bank management's planning and oversight of third-party arrangements. As such, banks should perform a thorough pre-analysis and risk assessment on each marketplace lending company with which it transacts business, whether acting as an institutional investor or as a strategic partner.[3]

A comprehensive list of risks associated with marketplace lending is not possible without an understanding of the arranged lending activity and the products offered. Although not a complete list, some risks include third-party, credit, compliance, liquidity, transaction, servicing, and bankruptcy risks. Before engaging in marketplace activity, banks should complete appropriate due diligence and ensure effective risk identification practices are in place as part of the risk assessment process.

Third-party risk can vary greatly depending on each third-party arrangement, elevating the importance for banks to conduct effective due diligence. Banks are encouraged to review the FDIC's Financial Institution Letter 44-2008 titled *Guidance for Managing Third-Party Risk*,[4] which discusses the critical elements to an effective third-party risk management process: (1) risk assessment, (2) due diligence in selecting a third party, (3) contract structuring and review, and (4) oversight.

Before engaging in any third-party arrangement, a financial institution should consider whether the proposed activities are consistent with the institution's overall business strategy and risk tolerances. Bank management is encouraged to develop a strong understanding of the marketplace lending company's business model, establish contractual agreements that protect the bank from risk, regularly monitor the marketplace service provider, and require the marketplace lending company to take corrective action

[3] See FIL-49-2015 "Advisory on Effective Risk Management Practices for Purchased Loans and Purchased Loan Participations", November 6, 2015 at https://www.fdic.gov/news/news/financial/2015/fil15049.html.

[4] See FIL-44-2008"Guidance for Managing Third-Party Risk," June 6, 2008 at https://www.fdic.gov/news/news/financial/2008/fil08044.html.

Marketplace Lending

continued from pg. 15

Due Diligence

- What duties does the bank rely on the marketplace lending company to perform?
- What are the direct and indirect costs associated with the program?
- Is the bank exposed to possible loss, and are there any protections provided to the bank by the marketplace lending company?
- What are the bank's rights to deny credit or limit loan sales to the marketplace lending company?
- How long will the bank hold the loan before sale?
- Who bears primary responsibility for consumer compliance requirements, and how are efforts coordinated?
- Is all appropriate and required product-related information effectively and accurately communicated to consumers?
- What procedures are in place to prevent identity theft and satisfy other customer identification requirements?
- What other risks is the bank exposed to through the marketplace arrangement?

when gaps or deficiencies occur. This due diligence may result in banks requiring policies and procedures from the marketplace lending company with respect to legal and regulatory compliance prior to the bank's investment or before any services are offered.

Some considerations include, but are not limited to, compliance with applicable federal laws such as lending laws, consumer protection requirements, anti-money laundering rules, and fair credit responsibilities along with adherence to any applicable state laws, licensing, or required registrations. As with any third-party arrangement, banks should monitor marketplace activities and expect marketplace servicers to undergo independent audits and take corrective action on audit exceptions as warranted. Failure to do so could expose a bank to substantial financial loss and an unacceptable level of risk.

For banks contemplating a funding relationship with a marketplace lending company, management should consider several issues that could affect the bank's risk profile. (See Due Diligence sidebar.) Banks also should consider validating the marketplace lending company's compliance with any applicable state or federal laws. Negotiated contracts should consider provisions allowing the financial institution the ability to control and monitor third-party activities (*e.g.*, underwriting guidelines, outside audits) and discontinue relationships if contractual obligations are not met.

Compliance risk is inherent in any marketplace lending activity. Banks are accountable for complying with all relevant consumer protection and fair lending laws and regulatory requirements and cannot assign this responsibility to a marketplace lending company. Although marketplace lending companies are required to comply with many of these requirements, well-run bank programs should include appropriate due diligence and ongoing monitoring to validate that the marketplace lending company demonstrates adherence to these requirements. Relevant laws may

include the Truth in Lending Act[5] (TILA) that, among other things, requires the disclosure of standardized loan terms and conditions at point of sale and in advertisements, and Section 5 of the Federal Trade Commission Act,[6] which prohibits unfair and deceptive acts or practices.

Consistent with the third-party risk guidance,[7] banks also should evaluate whether a bank-affiliated marketplace lending company complies with fair lending and other related laws including the Equal Credit Opportunity Act[8] (ECOA), which prohibits lenders from taking action related to any aspect of a credit transaction on the basis of race, color, religion, and other prohibited factors. Banks that partner with marketplace lending companies should exercise due diligence to ensure the marketplace loan underwriting and pricing policies and procedures are consistent with fair lending requirements.

Transaction risk is present given the potential for customer service problems or a marketplace lending company's failure to fulfill its duties as expected by the financial institution or its customers. Marketplace loans may be subject to high levels of transaction risk given the large volume of loans, handling of documents, and movement of loan funds between institutions or third-party originators. Banks should anticipate risks that could arise from problems with customer service, product delivery, technology failures, inadequate business continuity, and data security breaches.

Servicing risk exists given the pass-through nature of marketplace notes. The investor becomes a creditor to the marketplace lending company and has no access to the borrower. Therefore, if a marketplace lending company that services the loans becomes insolvent, investors may become exposed not only to bankruptcy risk but also servicing risk if the loan servicing process is disrupted. In bankruptcy, a marketplace lending company may be unable to fulfill its note servicing obligations to investors even if the borrowers continue to make timely payments.

Notwithstanding the fact that the loans in which they invested are fully performing, investors also may be exposed to losses if other creditors seek rights to these borrower payments in the bankruptcy proceeding. In the event a marketplace lending company becomes insolvent, investors line up in bankruptcy court to collect on monies owed on a pro rata basis, with no investor having any superior claim to a stream of payment than any other, and often times with interest halted once the bankruptcy proceedings commence.

At a minimum, banks that invest in marketplace loans should determine whether back-up servicing agreements are in place with an unaffiliated company before investment. Banks, as investors, committing significant capital to marketplace loans should assess the marketplace lending company's creditworthiness with consideration given to the business's solvency prior to investing the capital. Although this

[5] See the Truth in Lending Act at https://www.fdic.gov/regulations/laws/rules/6500-3200.html#fdic65001026.1.

[6] See Section 5 of the Federal Trade Commission Act at https://www.fdic.gov/regulations/laws/rules/8000-3000.html.

[7] Ibid.

[8] See the Equal Credit Opportunity Act at https://www.fdic.gov/regulations/laws/rules/6500-200.html.

continued from pg. 17

condition may not afford complete protection, it may mitigate some risk of loss.

Liquidity risk is present given the limited secondary market opportunities available for marketplace loans. Although there are a few known aftermarket providers, the secondary market for marketplace loans generally is limited with resale opportunities available only to a select few marketplace lending companies. Partner banks with loans in their marketplace pipeline may also experience liquidity risk for those pipeline loans that require funding.

Other considerations include compliance with other state and federal requirements, including anti-money laundering laws. The partner bank should evaluate the bank-affiliated marketplace company as it would any other customer or activity, and financial institutions investing in marketplace loans should exercise due diligence in evaluating appropriate compliance for any loan purchase.

A Supervisory Perspective

Before engaging in any marketplace lending third-party arrangement or balance sheet investment, a financial institution should ensure the proposed activities are consistent with the institution's overall business strategy and risk tolerances. FDIC examiners assess how financial institutions manage third-party relationships and other investments with marketplace lenders through review of bank management's record of and process for assessing, measuring, monitoring, and controlling the associated relationship and credit risks. The depth of the examination review depends on the scope of the activity and the degree of risk associated with the activity and the relationship. The FDIC considers the results of the review in its overall evaluation of management, including management's ability to effectively control risk.

FDIC examiners address findings and recommendations relating to an institution's third-party marketplace lender relationships and marketplace loan investments in the Report of Examination and within the ongoing supervisory process. Appropriate corrective actions, including formal or informal enforcement actions, may be pursued for deficiencies identified that pose significant safety and soundness concerns or result in violations of applicable federal or state laws or regulations.

Conclusion

Some banks are finding participation in the small but growing arena of marketplace lending to be an attractive source of revenue. With the market's infancy and its lack of performance history through a complete economic cycle, bank management should look beyond the revenue stream and determine whether the related risks align with the institution's business strategy. As noted earlier, financial institutions can manage the risks through proper risk identification, appropriate risk-management practices, and effective oversight. With the rapidly evolving landscape in marketplace lending, institutions should ascertain the degree of risk involved, remembering they cannot abrogate responsibility for complying with applicable rules and regulations.

Angela M. Herrboldt
Senior Examination Specialist
Division of Risk Management Supervision
aherrboldt@fdic.gov

Lending Viewpoint: Results from the FDIC's Credit and Consumer Products/ Services Survey

The lending landscape for banks continues to evolve. What hasn't changed is that the quality of a bank's loan portfolio continues to be of paramount importance to its long-term financial health. Thus, the assessment of lending and its related risks continues to be a key focus of the FDIC. This article describes the assessments of lending conditions and risks by FDIC risk-management examiners, based on Credit and Consumer Products/Services Surveys (Credit Surveys) submitted for examinations completed through the first half of 2015.

Lending Conditions

As measured by bank loan growth, recovery from the financial crisis and "great recession" continues to gather momentum. Total loans and leases held by FDIC-insured institutions rose to $8.5 trillion as of June 30, 2015, up 5.4 percent compared to one year prior.[1] This post-crisis rebound in lending volume is likely attributable, in part, to the low interest rate environment and a fair economic outlook encouraging individuals and businesses to tap into available credit. Not only is loan volume growing, but the proportion of institutions that are growing their loan portfolios is increasing. During the second quarter of 2015, 78 percent of banks grew their lending portfolios. This is up from about 74 percent the year prior.

Further, the rise in loan volume is broad-based. Acquisition, development, and construction (ADC) loans stood at $256 billion at mid-year 2015, an increase of nearly 15 percent from a year earlier. Commercial and industrial (C&I) loans were $1.8 trillion, an 8 percent increase from a year earlier. Consumer lending increased 4 percent to $1.4 trillion. Nonfarm, nonresidential commercial real estate loans increased 4 percent to about $1.2 trillion. In addition, 1-4 family residential mortgage loans held on balance sheet grew about 2 percent to a little less than $1.9 trillion. Unused loan commitments are nearly $6.7 trillion and are up 6 percent from a year earlier, indicating continued loan growth.

Loan performance continues to improve, reflecting the ongoing recovery in the nation's economy and bankers working through and/or selling off many of the problem legacy credits. The past due and nonaccrual (PDNA) ratio as of June 30, 2015, is 2.38 percent, a 67 basis point improvement from the year prior. During the 12-month period, the PDNA ratio improved for nearly all loan categories except the "All other loans and leases (including farm)" category, which only increased six basis points to 0.45 percent.

Given that borrowers generally do not immediately default after they have received a loan, metrics such as the PDNA ratio tend to be a lagging indicator of loan quality, especially in periods of rapid loan growth, and may not effectively provide banks and their regulators the lead time necessary to properly identify and address emerging credit risk. Accordingly, to facilitate earlier identification and

[1] Financial data and banking statistics for this article obtained from *Quarterly Banking Profile* for second quarters 2015, 2014, and 2013.

continued from pg. 19

Credit Survey History

The FDIC implemented the current Credit Survey in the fall of 2009. The Credit Survey is required to be completed by examiners at the conclusion of all risk management examinations. It solicits examiner assessments about the level of risk and quality of underwriting for loan portfolios and gathers information on new and evolving bank activities and products, among other items, with a focus on changes since the last examination.

Combining Credit Survey results with financial, economic, and examination data helps supervisory staff to better identify trends, perform forward-looking analyses, and prioritize the use of supervisory resources. In addition, the results are summarized for the banking industry in articles such as this one. Similar articles were published in the Winter 2010, Summer 2012, and Winter 2013 issues of *Supervisory Insights* (SIJ).

stronger tracking of lending conditions and risks, the FDIC reviews and analyzes examiners' responses to the Credit Surveys.[2]

Credit Survey Results

The observations reported by examiners in the Credit Survey reflect continuing improvement in the financial condition and overall risk profile of the banking industry. At the same time, Credit Survey results suggest that just as loan growth is returning, so to some extent are riskier lending practices. This development is not unusual in a banking cycle's upswing phase. Moreover, while selected indicators suggest the direction of risk is increasing, examiners are still typically reporting these indicators in the context of low to moderate levels of overall risk.

Overall loan portfolio risk

Credit Survey respondents continue to label the degree of risk in most lending portfolios as "low" to "moderate."[3] Reports of "high" risk portfolios declined substantially, from 23 percent of responses for the first half of 2013 to 14 percent of responses for the first half of 2015. For the first half of 2015, roughly 67 percent of Credit Surveys reported "moderate" risk in the loan portfolio, and 18 percent considered the risk level "low." Comparatively, for the first half of 2013, responses were 62 percent for "moderate" risk and 15 percent for "low" risk, respectively. The migration from the "high" risk level in the past few years may be due to the working through or selling-off of many problem credits and improvements in the economy, but perhaps also to tightening of underwriting standards in the aftermath of the recent financial crisis that was noted in prior Credit Survey results.[4]

When assessing the level of risk on a portfolio-type basis, an overall improving trend is noted for nearly all portfolios. Regardless, some portfolios are reporting a slight uptick in the proportion of "high" risk designations in the first half of 2015 (although the frequency of such designations remains well below those experienced with the recent crisis), suggesting that lending risk may be in the very early stages of increasing.

The Credit Survey results show the level of risk in the Agricultural loan portfolio has increased slightly during the past two years. Since the Credit Survey was implemented, the Agricultural loan portfolio generally had one of the highest percentages of "low" risk responses. During the past two years, there has been a slight

[2] Past SIJ articles summarizing Credit Survey results include: Jeffrey A. Forbes, Margaret M. Hanrahan, and Larry R. VonArb, "Lending Trends: Results from the FDIC's Credit and Consumer Products/Services Survey," Winter 2013; Jeffrey A. Forbes, Margaret M. Hanrahan, Andrea N. Plante, and Paul S. Vigil, "Results from the FDIC's Credit and Consumer Products/Services Survey: Focus on Lending Trends," Summer 2012; and Jeffrey A. Forbes, David P. Lafleur, Paul S. Vigil, and Kenneth A. Weber, "Insights from the FDIC's Credit and Consumer Products/Services Survey," Winter 2010.

[3] These descriptors apply only to banks with lending portfolios representing more than two percent of total assets ("de minimis portfolio rule").

[4] See articles in the Summer 2012 and Winter 2013 issues referenced in footnote 2.

but noticeable shift from "low" to "moderate" and "high" risk. Such a shift is to be expected as farm income has declined after several years of extraordinarily high levels. Although farm income has declined, farm debt levels remain manageable. That said, the level of risk within the Agricultural loan portfolio is dependent on how borrowers and bankers adjust to the lower levels of farm income. As a reminder, financial institutions are encouraged to work with borrowers experiencing financial difficulties. The FDIC will continue to closely monitor the agricultural economy and the quality and performance of the Agricultural loan portfolio.

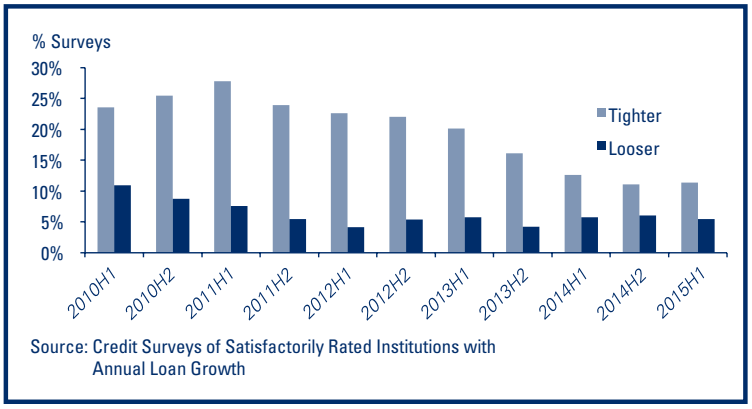
Regulators are also keeping a close eye on other portfolios, including ADC and commercial real estate (CRE) in general, which experienced significant loan losses in the recent financial crisis. Out-of-area lending and concentrations also remain on the regulatory radar and are discussed later in this article.

Underwriting

Prudent loan risk selection remains vital to a bank's financial health, and a bank's first line of defense against booking excessive credit risk is the initial underwriting process. For the first half of 2015, about 9 percent of Credit Surveys reported "generally liberal" underwriting in one or more portfolios.[5] This is a slight uptick from the 8 percent reported in the second half of 2014, but is still a lower incidence of "generally liberal" underwriting practices than reported in all other prior six-month periods. The portfolio most often cited as having "generally liberal" underwriting is the consumer portfolio (6 percent for the first half of 2015), with the C&I portfolio ranking second (6 percent), and the ADC portfolio ranking third (5 percent).

The Credit Surveys indicate that examiners are typically observing no material changes in underwriting. This has remained the case during the past five years (see Chart 1). When examiners have observed a material change in loan underwriting practices, they more often report tightening than easing, again a trend that has persisted during this period. Another consistent trend is that the proportion of banks where examiners have reported tighter standards has generally declined since 2011, leading to an increase in "no material change" observations. Whether tightening or relaxing, the preponderance of the material underwriting changes continues to be characterized by Credit

Chart 1: Changes in Underwriting Standards



Source: Credit Surveys of Satisfactorily Rated Institutions with Annual Loan Growth

[5] De minimis portfolio rule (see footnote 3).

continued from pg. 21

Survey respondents as "moderate" versus "substantial."

On an aggregate portfolio basis, changes in economic conditions and responses to regulatory observations and recommendations are generally the most common factors reported to be influencing changes in underwriting practices. Lesser, but still important, reported factors include competitive forces, changes in management, and growth goals.

The Credit Survey results described thus far have indicated that in broad terms, the banking industry continues to exhibit a lower risk profile than it did coming out of the financial crisis, and that examiners generally are describing the overall level of lending risks as moderate. However, as noted earlier, Credit Survey responses also indicate that risks related to selected portfolios or lending practices may be starting to increase. Some of these issues are described below.

About 10 percent of the applicable surveys for satisfactorily rated banks during the past 18 months reported those banks loosening at least one of the specified types of underwriting standards for C&I and permanent CRE loans. Reducing the spread between the loan rate and cost of funds is the most frequently reported area of loosening for this portfolio, followed by increasing the maximum maturity of loans.

As mentioned previously, ADC lending is on the rise, albeit from a lower base following a post-crisis retrenchment of this sector. Examiners noted higher-risk ADC lending activities in about 22 percent of applicable Credit Surveys for satisfactorily rated banks during the past 18 months. This remains elevated compared to other loan portfolio types. Speculative lending is the most frequently reported higher-risk activity. It is followed by repayment source themes: funding of ADC loans without consideration of repayment sources other than the sale of collateral and failing to verify the quality of alternative repayment sources.

The agricultural economy has been strong; however, real net farm income has been declining since the 2013 peak. The increases in the overall level of risk in agricultural loan portfolios noted earlier is probably more attributable to these economic developments rather than to weak lending practices, since for most banks the Credit Survey results do not show an increase in higher-risk agricultural lending practices. For some banks, however, riskier practices are being reported. One sign of a weaker agricultural economy is an increase in Credit Surveys reporting institutions that are extending or renewing unpaid production/operating loans structured to be paid in full at maturity and not secured by marketable collateral, e.g. carryover debt. Other agricultural lending practices reported to be on the rise at some banks, although less frequently reported than carryover debt, are making livestock loans without documenting livestock inspections and lending to borrowers who lack documented financial strength to support the loan.

Lending Products and Strategies

As the banking industry continues its rebound from the crisis and banks look to combat compressed net interest margins, banks are growing

loans, sometimes by way of offering new products or expanding existing lending strategies. Credit Surveys reporting new or evolving products, activities, or strategies that could pose risks to the institution increased from about 10 percent between 2010 and 2011 to roughly 13 percent in 2014 and 2015. Examples of the most frequently cited new and emphasized lending products in the Credit Surveys include purchasing loans (including out-of-area, participations, and Shared National Credits); ADC and CRE lending; C&I lending; and Small Business Administration lending.

Along with the uptick in new and emphasized lending products, Credit Survey results show that examiners view the risks associated with loan growth as somewhat greater than in past Credit Surveys. Specifically, for the first half of 2015, 47 percent of Credit Surveys reported the risk associated with loan growth and/or changes in lending activities as "moderate" or "high." This is up from 43 percent two years prior and from 45 percent one year ago.

A variety of reasons for "high" risk designations was observed. For satisfactorily rated institutions, many comments focused on the rate of growth, with CRE/ADC and residential real estate being the most frequently cited. Credit administration, merger/acquisition activity, and participation or brokered loans were also repeatedly cited as risk factors.

Out-of-Area Lending

Many banks, such as some in markets with sluggish loan demand, consider out-of-area lending as a way to grow loans. Over time, advances in technology and partnerships with third parties have made out-of-area loans more readily available to banks. As discussed in the Winter 2013 SIJ article, out-of-area lending grew dramatically in the years before the crisis, and those loans often were purchased whole or in participations underwritten by other financial institutions. Many failed banks had relatively large portfolios of out-of-area loans that deteriorated quickly, and the deterioration was exacerbated by weak due diligence at origination, lack of knowledge about the area where the loan was made, and reliance on a third party that poorly managed the credit. The Winter 2013 SIJ article also suggested that institutions were implementing lessons learned from the crisis as fewer banks were making out-of-area loans at that time.

More recently, Credit Survey results show that trend may be reversing. Reports of out-of-area lending increased in the first half of 2015 (see Chart 2). About 19 percent of Credit Surveys for this period[6] report out-of-area lending as a standard practice or a practice engaged in frequently enough to warrant notice. This is up from 15 percent for the first half of 2014 and from 14 percent for the first half of 2013. Although out-of-area lending is trending up, it has not reached the levels reported for 2009 to 2012.

In January 2015, the Credit Survey question for out-of-area lending was revised, in part, to separate the lending categories into direct and indirect lending.[7] Commercial lending (including CRE/ADC) is the loan portfolio

[6] Ibid.

[7] Indirect lending includes purchased out-of-area participations and whole loans and all loans purchased from non-FDIC-insured entities regardless of the location.

continued from pg. 23

Chart 2: Out-of-Area Lending Trended Up in 2015

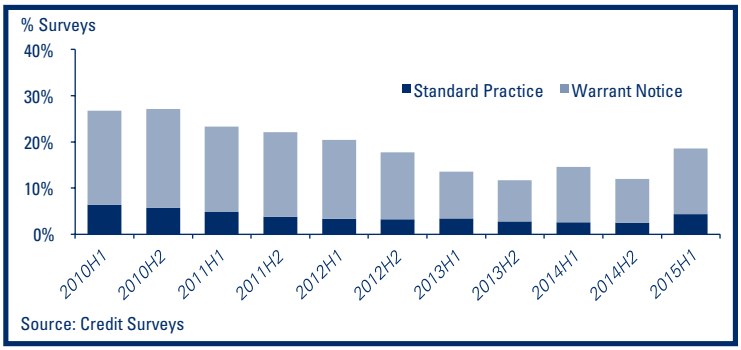
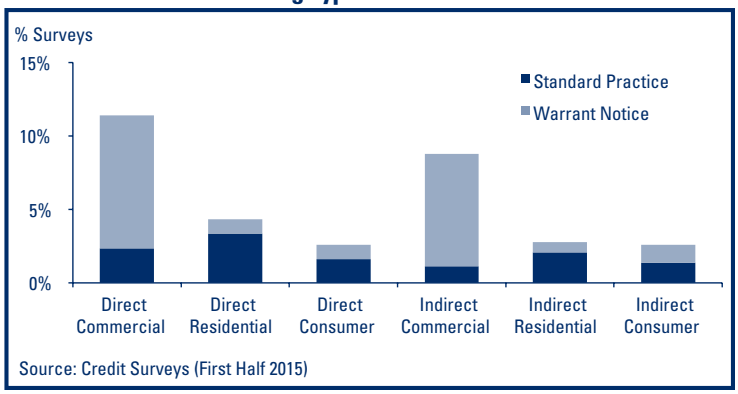


Chart 3: Out-of-Area Lending Type



most often associated with out-of-area lending, on both direct and indirect bases. In 13 percent of Credit Surveys for the first half of 2015, institutions were identified as being engaged in direct or indirect out-of-area lending for their commercial portfolios as a standard practice or frequently enough to warrant notice. The percentages reported for residential and consumer portfolios were much lower (see Chart 3). Depending on the portfolio type, approximately 26 to 29 percent of the institutions identified as engaged in out-of-area lending are reported to be engaged in both direct and indirect out-of-area lending.

In early November 2015, the FDIC issued FIL-49-2015 to update information contained in the FDIC Advisory on Effective Credit Risk Management Practices for Purchased Loan Participations (FIL-38-2012). The updated advisory addresses purchased loans and loan participations and reminds FDIC-supervised institutions of the importance of underwriting and administering purchased credits as if the loans were originated by the purchasing institution. The updated advisory also reminds institutions that third-party arrangements to facilitate loan and loan participation purchases should be managed by an effective third-party risk management process.

Concentrations

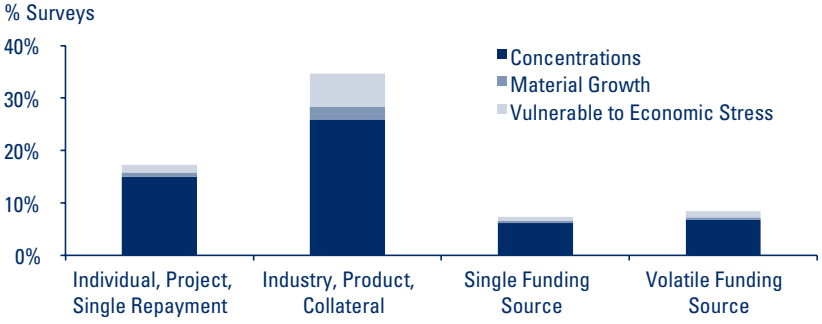
Loan growth has the potential to create or exacerbate concentrations of credit and/or funding. The FDIC recognizes that concentration risk is a reality for many institutions, and is often a reflection of local econo-

mies, borrowing needs, and market conditions. Concentrations are not inherently problematic, but the associated risks need to be well-managed. As discussed in the Winter 2013 SIJ article, ineffective risk management of growing concentrated portfolios has been a key contributor to asset problems in many banking crises. As such, the FDIC continues to closely track trends in concentrations.

About 55 percent of Credit Surveys for the first half of 2015 reported at least one credit and/or funding concentration. Moreover, many institutions that have concentrated loan portfolios are growing those portfolios. Based on June 30, 2015, Call Report data, about 49 percent of institutions with one or more loan portfolios that exceed 300 percent of total capital[8] grew such a portfolio over 10 percent.[9]

In the fourth quarter of 2013, the Credit Survey question for credit and funding concentrations was revised to provide more granular data on concentrations including, among other items, type. Chart 4 summarizes concentration types on a broad category basis as reported through the Credit Survey. More specifically, the most frequently cited credit concentrations in the Credit Survey results are CRE/ADC, individual borrower, agriculture, residential/multi-family real estate, hospitality, and out-of-area/participations. On the funding side, the most frequently cited concentrations are brokered deposits, borrowings/wholesale funds, large deposits, public funds, and internet/listing service deposits. As indicated in the Chart, survey responses characterized a subset of these concentrations as displaying material growth or vulnerability to economic stress.

Chart 4: Credit and Funding Concentrations



Source: Credit Surveys (First Half 2014 through First Half 2015)

Outlook and Viewpoint

The lending environment will continue to change. Banks are growing loan portfolios, and there may be early signs of emerging risk. In the current environment, banks are facing strong competition, earnings pressure, and increasing deposits. How well banks manage loan growth, concentrations, funding, and new products or services will be critical to their successful operation going forward. As banks revisit risk tolerances and market strategies to remain competitive, management should remember that prudent risk selection and careful monitoring of the lending portfolio are integral components of a well-managed institution. When assessing proposed and new products and activities, considerations should include matters such as whether the bank understands the risks associated with the market or product, whether pricing is appropriate for any increased risk, and whether the

[8] For ADC lending, 100 percent of total capital is used.

[9] For institutions with more than one portfolio exceeding the threshold, the highest growth rate is used.

continued from pg. 25

proper resources, including technology and staffing, are available.

The data obtained from the Credit Surveys are valuable to the supervisory process. The FDIC will continue to evaluate the Credit Survey data along with other sources of information to proactively identify and address the continued evolution of lending practices and risks at the banks we supervise.

Lisa A. Garcia
Senior Examination Specialist
Division of Risk Management Supervision
ligarcia@fdic.gov

Kenneth A. Weber
Senior Quantitative Risk Analyst
Division of Risk Management Supervision
kweber@fdic.gov

Overview of Selected Regulations and Supervisory Guidance

This section provides an overview of recently released regulations and supervisory guidance, arranged in reverse chronological order. Press Release (PR) and Financial Institution Letter (FIL) designations are included so the reader can obtain more information.

ACRONYMS and DEFINITIONS	
CFPB	Consumer Financial Protection Bureau
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FRB	Federal Reserve Board
NCUA	National Credit Union Administration
OCC	Office of the Comptroller of the Currency
Federal bank regulatory agencies	FDIC, FRB, and OCC
Federal financial institution regulatory agencies	CFPB, FDIC, FRB, NCUA, and OCC

Subject	Summary
FDIC Issues Additional Cybersecurity Awareness Resources (FIL-55-2015, November 23, 2015)	The FDIC is adding to its cybersecurity awareness resources for financial institutions. The new resources include a Cybersecurity Awareness video and three vignettes for the Cyber Challenge, which consist of exercises that encourage discussions of operational risk issues and the potential impact of information technology (IT) disruptions on common banking functions. See https://www.fdic.gov/news/news/financial/2015/fil15055.html
FFIEC Issues Updated Management Booklet as Part of IT Examination Handbook Series (FIL-54-2015, November 20, 2015)	The FFIEC has issued a revised "Management" booklet that provides guidance to assist examiners in evaluating the IT governance at financial institutions and service providers. The booklet is part of the IT Examination Handbook series. See https://www.fdic.gov/news/news/financial/2015/fil15054.html
FDIC Board Approves Proposed Rule to Increase Deposit Insurance Fund To Statutorily Required Level (FIL-53-2015, November 17, 2015)	On October 22, 2015, the FDIC Board of Directors adopted a proposal to increase the Deposit Insurance Fund to the statutorily required minimum level of 1.35 percent. The proposed rule would impose on banks with at least $10 billion in assets a surcharge of 4.5 cents per $100 of their assessment base, after making certain adjustments. The FDIC expects the reserve ratio would likely reach 1.35 percent after approximately two years of payments of the proposed surcharges. Comments on the proposed rule are due January 5, 2016. See https://www.fdic.gov/news/news/financial/2015/fil15053.html

Regulatory and Supervisory Roundup

continued from pg. 27

Subject	Summary
FDIC Clarifies its Approach to Banks Offering Certain Products and Services to Non-Bank Payday Lenders (FIL-52-2015, November 16, 2015)	The FDIC is reissuing its 2005 *Payday Lending Guidance* (FIL-14-2005) to ensure bankers and others are aware that it does not apply to banks offering products and services, such as deposit accounts and extensions of credit, to non-bank payday lenders. Financial institutions that can properly manage customer relationships and effectively mitigate risks are neither prohibited nor discouraged from providing services to any category of business customers or individual customers operating in compliance with applicable state and federal laws. See https://www.fdic.gov/news/news/financial/2015/fil15052.html
FDIC Seeking Comment on Frequently Asked Questions Regarding Identifying, Accepting, and Reporting Brokered Deposits (FIL-51-2015, November 13, 2015)	The FDIC is seeking comment on a proposed update to a series of frequently asked questions and an accompanying introductory letter regarding identifying, accepting and reporting brokered deposits that were issued in January 2015 through FIL-2-2015. Comments on the proposed update are due December 28, 2015. See https://www.fdic.gov/news/news/financial/2015/fil15051.html
Agencies Announce Final EGRPRA Outreach Meeting (PR-90-2015, November 13, 2015)	The federal banking agencies will hold the final outreach meeting on Wednesday, December 2, 2015, at the FDIC in Arlington, VA, as part of their regulatory review under the *Economic Growth and Regulatory Paperwork Reduction Act of 1996 (EGRPRA)*. The meeting will feature panel presentations by bankers and consumer and community groups. See https://www.fdic.gov/news/news/press/2015/pr15090.html
FDIC Issues Guidance on Capital Treatment of Certain Investments in Covered Funds (FIL-50-2015, November 6, 2015)	The FDIC is issuing guidance to FDIC-supervised institutions to clarify the interaction between the regulatory capital rule and the final rule implementing Section 13 of the *Bank Holding Company Act* (*"Volcker Rule"*) with respect to the appropriate capital treatment for investments in certain private equity funds and hedge funds ("covered funds"). See https://www.fdic.gov/news/news/financial/2015/fil15050.html
FDIC Issues Advisory on Effective Risk Management Practices for Purchased Loans and Purchased Loan Participations (FIL-49-2015, November 6, 2015)	The FDIC is issuing an Advisory to update information contained in the *FDIC Advisory on Effective Credit Risk Management Practices for Purchased Loan Participations* (FIL-38-2012). The updated Advisory addresses purchased loans and loan participations and reminds FDIC-supervised institutions of the importance of underwriting and administering these purchased credits as if the loans were originated by the purchasing institution. The updated Advisory also reminds institutions that third-party arrangements to facilitate loan and loan participation purchases should be managed by an effective third-party risk management process. See https://www.fdic.gov/news/news/financial/2015/fil15049.html

Subject	Summary
Shared National Credits Review Notes High Credit Risk and Weaknesses Related to Leveraged Lending and Oil and Gas (PR-89-2015, November 5, 2015)	Credit risk in the Shared National Credit portfolio remained at a high level, according to an annual review of large shared credits released by the federal bank regulatory agencies. The review found that leveraged lending transactions originated in the past year continue to exhibit weak structures. The review also noted an increase in weakness among credits related to oil and gas exploration, production, and energy services following the decline in energy prices since mid-2014. See https://www.fdic.gov/news/news/press/2015/pr15089.html
Five Federal Agencies Finalize Swap Margin Rule (PR-86-2015, October 30, 2015)	The FDIC, OCC, FRB, Farm Credit Administration, and Federal Housing Finance Agency issued a final rule to establish capital and margin requirements for swap dealers, major swap participants, security-based swap dealers, and major security-based swap participants regulated by one of the agencies ("covered swap entities"), as required by the *Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act)*. See https://www.fdic.gov/news/news/press/2015/pr15086.html
FDIC Hosts Industry Teleconference in Recognition of Cybersecurity Awareness Month (FIL-48-2015, October 23, 2015)	In recognition of President Obama's designation of October as National Cybersecurity Awareness month, the FDIC is hosting an informational call for FDIC-supervised institutions on October 28, 2015. The call will address and discuss the FDIC's regulatory expectations regarding cybersecurity preparedness and allow industry participants to ask questions. See https://www.fdic.gov/news/news/financial/2015/fil15048.html
FDIC Provides Guidance for Financial Institutions Implementing the Truth in Lending Act and Real Estate Settlement Procedures Act Integrated Disclosure Rule (FIL-43-2015, October 2, 2015)	The FDIC is providing guidance on its supervisory expectations in connection with examinations of financial institutions for compliance with the *Truth in Lending Act – Real Estate Settlement Procedures Act Integrated Disclosure Rule*, which is effective October 3, 2015. See https://www.fdic.gov/news/news/financial/2015/fil15043.html
FDIC to Conduct Deposit Insurance Coverage Seminars (FIL-38-2015, September 14, 2015)	The FDIC will conduct four live seminars on FDIC deposit insurance coverage for bank employees and bank officers between September 24, 2015, and December 2, 2015. In addition, the FDIC has developed three deposit insurance coverage seminars for bank officers and employees, which are now available on FDIC's YouTube channel. The live and the YouTube deposit insurance coverage seminars will provide bank employees with an understanding of how to calculate deposit insurance coverage. See https://www.fdic.gov/news/news/financial/2015/fil15038.html
FDIC Updates its Money Smart Financial Education Program for Consumers/Individuals with Visual Disabilities (PR-79-2015, October 5, 2015)	The FDIC announced two resources tailored to meet the financial education needs of individuals with visual disabilities. The FDIC's *Money Smart* curriculum for adults is available in Braille and Large Print. In addition, the latest version of the *Money Smart* Podcast Network—the audio version of *Money Smart*— is available in Spanish. See https://www.fdic.gov/news/news/press/2015/pr15079.html

Regulatory and Supervisory Roundup

continued from pg. 29

Subject	Summary
Agencies Announce EGRPRA Outreach Meeting in Chicago (PR-75-2015, September 28, 2015)	The federal bank regulatory agencies will hold an outreach meeting on Monday, October 19, 2015, at the Federal Reserve Bank of Chicago as part of their regulatory review under *EGRPRA*. The meeting will feature panel presentations by bankers and consumer and community groups. See https://www.fdic.gov/news/news/press/2015/pr15075.html
FDIC Consumer Newsletter Features Tips on Choosing and Using Bank "Rewards" (PR-68-2015, August 27, 2015)	The Summer 2015 edition of *FDIC Consumer News* features tips when choosing a bank rewards program tied to credit or debit cards that earn points or provide cash back benefits. The edition also has articles on mobile financial services, automated teller machines, credit scores, reverse mortgages, and deposit insurance. See https://www.fdic.gov/news/news/press/2015/pr15068.html
Supervisory Insights Journal Released (FIL-36-2015, August 24, 2015)	The Summer 2015 issue of *Supervisory Insights* features two articles of interest to examiners, bankers, and supervisors. One article highlights the critical role of corporate governance and strategic planning in navigating a challenging operating environment. The second article discusses the new requirements related to bank investment in securitizations as a result of the enactment of the *Dodd-Frank Act*. See https://www.fdic.gov/news/news/financial/2015/fil15036.html
Agencies Issue Final Rule on Loans in Special Flood Hazard Areas (FIL-32-2015, July 21, 2015)	The FDIC, OCC, FRB, NCUA, and Farm Credit Administration approved the issuance of a joint final rule to amend their respective regulations regarding loans in special flood hazard areas. The final rule incorporates and implements certain provisions in the *Biggert-Waters Flood Insurance Reform Act of 2012 (BW Act)* and the *Homeowner Flood Insurance Affordability Act of 2014 (HFIAA)* regarding detached structures, force placement of flood insurance, and escrowing of flood insurance premiums and fees. See https://www.fdic.gov/news/news/financial/2015/fil15032.html
Agencies Release List of Distressed or Underserved Geographies (PR-59-2015, July 8, 2015)	The federal bank regulatory agencies announced the availability of the 2015 list of distressed or underserved nonmetropolitan middle-income geographies, where revitalization or stabilization activities will receive *Community Reinvestment Act* consideration as community development. See https://www.fdic.gov/news/news/press/2015/pr15059.html
Agencies Post Public Sections of Resolution Plans (PR-58-2015, July 6, 2015)	The FDIC and FRB posted the public portions of annual resolution plans for 12 large financial firms. Each plan must describe the company's strategy for rapid and orderly resolution under the U.S. Bankruptcy Code in the event of material financial distress or failure of the company. See https://www.fdic.gov/news/news/press/2015/pr15058.html

Subject	Summary
Agencies Announce EGRPRA Outreach Meeting (PR-57-2015, July 6, 2015)	The federal bank regulatory agencies will hold an outreach meeting on Tuesday, August 4, 2015, at the Federal Reserve Bank of Kansas City as part of their regulatory review under *EGRPRA*. The meeting will focus on rural banking issues and will feature panel presentations by industry participants and consumer and community groups. See https://www.fdic.gov/news/news/press/2015/pr15057.html
FDIC Announces Meeting of Advisory Committee on Community Banking (PR-56-2015, July 6, 2015)	The FDIC announced that its Advisory Committee on Community Banking will meet on Friday, July 10. Staff will provide an update on the FDIC's Community Banking Initiatives and discuss a number of issues, including examination frequency and offsite monitoring; call report streamlining; the cybersecurity assessment tool; high volatility commercial real estate loans; and the review of banking regulations under *EGRPRA*. See https://www.fdic.gov/news/news/press/2015/pr15056.html
FDIC Issues Cybersecurity Assessment Tool (FIL-28-2015, July 2, 2015)	The FDIC, in coordination with the other members of the FFIEC, is issuing the FFIEC Cybersecurity Assessment Tool to help institutions identify their cybersecurity risks and determine their preparedness. See https://www.fdic.gov/news/news/financial/2015/fil15028.html
FDIC Releases Interagency Examination Procedures for Truth in Lending Act and Real Estate Settlement Procedures Act Mortgage Rules (FIL-27-2015, June 30, 2015)	The FDIC released revised interagency examination procedures for the new *Truth in Lending Act (TILA) - Real Estate Settlement Procedures Act (RESPA) Integrated Disclosure Rule (TRID Rule)*, as well as amendments to other provisions of *TILA Regulation Z* and *RESPA Regulation X*. The CFPB issued a proposal for a TRID Rule effective on October 3, 2015. See https://www.fdic.gov/news/news/financial/2015/fil15027.html
Agencies Issue Host State Loan-to-Deposit Ratios. (PR-54-2015, June 29, 2015)	The federal bank regulatory agencies issued the host state loan-to-deposit ratios they will use to determine compliance with Section 109 of the *Riegle-Neal Interstate Banking and Branching Efficiency Act of 1994*. These ratios update data released on July 2, 2014. See https://www.fdic.gov/news/news/press/2015/pr15054.html
Agencies Announce Approval of Final Rule that Modifies Regulations that Apply to Loans Secured by Properties in Flood Hazard Areas. (PR-52-2015, June 22, 2015)	The FDIC, OCC, FRB, NCUA, and Farm Credit Administration announced the approval of a joint final rule that modifies regulations that apply to loans secured by properties located in special flood hazard areas. The final rule implements provisions of the *HFIAA* relating to the escrowing of flood insurance payments and the exemption of certain detached structures from the mandatory flood insurance purchase requirement. The final rule also implements provisions in the *BW Act* relating to the force placement of flood insurance. See https://www.fdic.gov/news/news/press/2015/pr15052.html

Federal Deposit Insurance Corporation

Washington, DC 20429-9990

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

FIRST CLASS MAIL

Postage &
Fees Paid
FDIC
Permit No. G-36

Subscription Form

To obtain a subscription to ***Supervisory Insights***, please print or type the following information:

Institution Name _____

Contact Person _____

Telephone _____

Street Address _____

City, State, Zip Code _____

Please fax or mail this order form to: FDIC Public Information Center
3501 North Fairfax Drive, Room E-1022
Arlington, VA 22226
Fax Number (703) 562-2296

Subscription requests also may be placed by calling 1-877-ASK-FDIC or 1-877-275-3342
or go to https://service.govdelivery.com/service/multi_subscribe.html?code=USFDIC