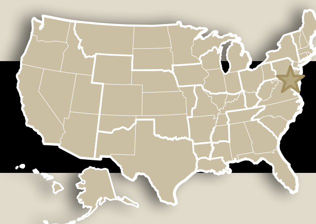
FEDERAL RESERVE SYSTEM

COMMUNITY BANKING
CONNECTIONS®
A SUPERVISION AND REGULATION PUBLICATION

Second Quarter 2015



View from Washington

Some Thoughts on Community Banking: A Conversation with Chair Janet Yellen

Throughout her career at the Federal Reserve, Janet Yellen has recognized the important role that community banks play in the U.S. economy. *Community Banking Connections* Advisory Board members sat down with Chair Yellen to get further insight from her on the benefits of community banking and the various challenges that these institutions face today.

Advantages and Challenges Facing Community Banks

Q Why are community banks important to the economy?

A I believe a healthy financial system relies on institutions of different sizes performing a variety of functions and serving a range of customer needs. Community banks[1] play an important role in our national economy. For one thing, they help to reduce the number of underbanked customers, especially in rural areas that may not be served by larger banking organizations. Community banks also help to keep their local communities vibrant and growing by providing financial services to local consumers and businesses.

Chair Janet Yellen

Community banks understand their customers' needs and local economic conditions, and, as a result, they sometimes can be more responsive to local lending requests than large multistate banks. Because they know their customers so well, community banks often will consider a broader range of fac-

continued on page 8

[1] For supervisory purposes, the Federal Reserve uses the term "community banking organization" to describe a state member bank and/or holding company with $10 billion or less in total consolidated assets.

INSIDE

What Community Bankers Should Know About Virtual Currencies 2
Managing the Risk of Unauthorized Payments from Business Bank Accounts 4
What Explains Low Net Interest Income at Community Banks? 6
Regulatory Recap 13
FedLinks 17
D.C. Updates 21
To Keep You Informed 23

What Community Bankers Should Know About Virtual Currencies

by Wallace Young, Director, Federal Reserve Bank of San Francisco

Virtual currencies are growing in popularity. While the collective value of virtual currencies is still a fraction of the total U.S. dollars in circulation, the use of virtual currencies as a payment mechanism or transfer of value is gaining momentum. Additionally, the number of entities (issuers, exchangers, and intermediaries, to name just a few) that engage in virtual currency transactions is increasing, and these entities often need access to traditional banking services. Providing banking services to these entities presents some unique risks and challenges. This article identifies some of the more significant risks that community bank management teams should consider before engaging in this banking activity.

Bitcoin Leads the Way

Launched in 2009, Bitcoin is currently the largest and most popular virtual currency. However, many other virtual currencies have emerged over the past several years, such as Litecoin, Dogecoin, and Peercoin.[1] Meanwhile, even more virtual currencies are being developed; one of these is Dash (formerly Darkcoin), which offers even more anonymity and privacy than that provided by Bitcoin. Another new and specialized virtual currency is DopeCoin, which was developed for those who wish to purchase marijuana, either legally or illegally.

The virtual currency landscape includes many participants, from the merchant that accepts the virtual currency, to the intermediary that exchanges the virtual currency on behalf of the merchant, to the exchange that actually converts the virtual currency to real currency, to the electronic wallet provider that holds the virtual currency on behalf of its owner. Accordingly, opportunities abound for community banks to provide services to entities engaged in virtual currency activities. Eventually, it is also possible that community banks may find themselves holding virtual currency on their own balance sheets.

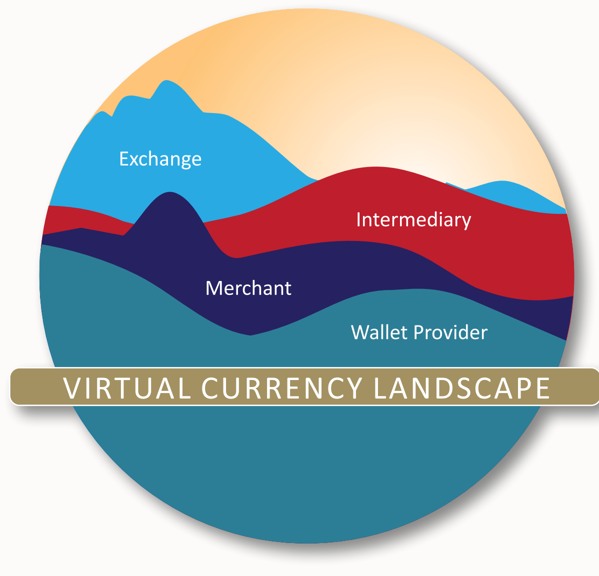
[1] Bitcoin and the other more recent virtual currencies are all examples of decentralized systems that allow for exchanges of value without the intermediation of a third party, are not owned or run by anyone, and operate on peer-to-peer networks. There have also been other types of centralized virtual currencies, such as the now-defunct Liberty Reserve and E-gold and the still-operating WebMoney. Centralized virtual currencies are characterized by a central clearing and access system usually owned and operated by a single administrator. For purposes of this article, virtual currency refers to decentralized virtual currencies, such as Bitcoin.

Community Banking Connections is published quarterly and is distributed to institutions supervised by the Federal Reserve System. Current and past issues of *Community Banking Connections* are available at www.communitybankingconnections.org or www.cbcfrs.org. Suggestions, comments, and requests for back issues are welcome in writing (editor@communitybankingconnections.org) or by telephone at 800-372-0248.

Editor: **Hilda Guay**
Project Manager: **Donna Gullé**
Designer: **Dianne Hallowell**
Advisory Board: **Jackie Brunmeier**, Assistant Vice President, Supervision, Regulation, and Credit, FRB Minneapolis, **Anthony Cain**, Manager, Supervisory Oversight, Division of Banking Supervision and Regulation, Board of Governors, **Cynthia Course**, Director, Office of the Director, Financial Institution Supervision and Credit, FRB San Francisco, **Mark Davenport**, Banking Supervisor, Supervision and Regulation, FRB Cleveland, **Joan Fischmann**, Assistant Vice President and Regional Director, Supervision and Regulation, FRB Chicago, **Jinai Holmes**, Senior Supervisory Financial Analyst, Policy Implementation and Effectiveness, Division of Banking Supervision and Regulation, Board of Governors, **Tara Humston**, Assistant Vice President, Supervision and Risk Management, FRB Kansas City, **Laura Macedo**, Senior Supervisory Financial Analyst, Supervisory Oversight, Division of Banking Supervision and Regulation, Board of Governors, **T. Kirk Odegard**, Assistant Director, Policy Implementation and Effectiveness, Division of Banking Supervision and Regulation, Board of Governors, **Erik Soell**, Program Director, Community Bank Research and Outreach, FRB St. Louis, **Constance Wallgren**, Vice President and Chief Examinations Officer, Supervision, Regulation and Credit, FRB Philadelphia, **Lauren Ware**, Assistant Vice President, Supervision, Regulation, and Credit, FRB Richmond, **Richard Watkins**, Deputy Associate Director, Supervisory Oversight, Division of Banking Supervision and Regulation, Board of Governors

The analyses and conclusions set forth in this publication are those of the authors and do not necessarily indicate concurrence by the Board of Governors, the Federal Reserve Banks, or the members of their staffs. Although we strive to make the information in this publication as accurate as possible, it is made available for educational and informational purposes only. Accordingly, for purposes of determining compliance with any legal requirement, the statements and views expressed in this publication do not constitute an interpretation of any law, rule, or regulation by the Board or by the officials or employees of the Federal Reserve System.

Copyright 2015 Federal Reserve System. This material is the intellectual property of the Federal Reserve System and cannot be copied without permission.



The Virtual Currency Landscape

Virtual currencies such as Bitcoin are digital representations of value that function as a medium of exchange, a unit of account, and/or a store of value.[2] In many cases, virtual currencies are "convertible" currencies; they are not legal tender, but they have an equivalent value in real currency. In terms of value, Bitcoin is the most prominent virtual currency. As of late January 2015, one bitcoin equaled roughly $207 (though the value is volatile), and all bitcoins in circulation totaled $2.85 billion. The next largest virtual currency was Ripple ($441.4 million in aggregate), followed by Litecoin ($43.2 million), PayCoin ($37.8 million), and BitShares ($24.2 million). Note that despite what seems to be a tremendous interest in virtual currencies, their overall value is still extremely small relative to other payment mechanisms, such as cash, checks, and credit and debit cards. For example, in 2013, U.S. credit and debit cards accounted for over $4 trillion in spending.[3]

For Bitcoin, the landscape also includes virtual currency exchangers (including Coinbase and Bitstamp), as well as wallet providers (such as Coinbase, Coinkite, and BitAddress) that hold the bitcoins until they are converted or otherwise transferred. Then, there are intermediaries such as BitPay, which provide the technology and services to merchants that accept bitcoins in exchange for goods and services. Of course, these merchants are also important participants; according to recent estimates, there are now over 100,000 merchants around the world that accept Bitcoin.[4] That is still a small number, but many large, high-profile companies such as Overstock, Dell, and Microsoft now accept Bitcoin, and it seems likely the number of merchants that accept virtual currency (Bitcoin in particular) will increase.

Compliance Risk

Considering the virtual currency landscape, what important risks should community bankers consider? The most significant is compliance risk, a subset of legal risk. Specifically, virtual currency administrators or exchangers may present risks similar to other money transmitters, as well as presenting their own unique risks. Quite simply, many users of virtual currencies do so because of the perception that transactions conducted using virtual currencies are anonymous. The less-than-transparent nature of the transactions may make it more difficult for a financial institution to truly know and understand the activities of its customer and whether the customer's activities are legal. Therefore, these transactions may present a higher risk for banks and require additional due diligence and monitoring.

More technically, the U.S. Financial Crimes Enforcement Network (FinCEN) has designated virtual currency exchanges and administrators as money transmitters.[5] Accordingly, banks are expected to manage the risks associated with the accounts of virtual currency administrators and exchanges just as they would any other money transmitter. The *Bank Secrecy Act/ Anti-Money Laundering (BSA/AML) Examination Manual,*[6] maintained and published by the Federal Financial Institutions Examination Council (FFIEC), contains a more detailed discussion of customer due diligence and enhanced due diligence expectations, including for money transmitter customers.

continued on page 12

[2] Internal Revenue Service, Notice 2014-21, March 25, 2014, available at www.irs.gov/pub/irs-drop/n-14-21.pdf.

[3] See *The Nilson Report*, February 18, 2014.

[4] Anthony Cuthbertson, "Bitcoin Now Accepted by 100,000 Merchants Worldwide," *International Business Times*, February 4, 2015.

[5] Specifically, FinCEN stated in 2013 guidance that "an administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN's regulations, unless a limitation to or exemption from the definition applies to the person." See Department of the Treasury, Financial Crimes Enforcement Network, FIN-2013-G001, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013, available at www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf.

[6] See www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm.

Managing the Risk of Unauthorized Payments from Business Bank Accounts

by Kenneth Benton, Senior Consumer Regulations Specialist, Federal Reserve Bank of Philadelphia

Unauthorized electronic payments from business bank accounts are a growing concern for banks, businesses, and the general public. Criminals are using a variety of techniques, such as phishing e-mails and malware, to take control of business accounts to initiate payments to an accomplice or a foreign account. According to the 2015 survey of the Association for Financial Professionals, 27 percent of respondent organizations were affected by wire transfer fraud (a nearly 100 percent increase from the 2014 survey), and 10 percent were affected by automated clearing house (ACH) credit fraud (fraud involving an ACH payment order initiated by the person sending the payment).[1]

For example, in June 2012, a law firm with a real estate escrow account had its computer system compromised and its banking credentials stolen, which resulted in $1.66 million in unauthorized wire transfers.[2] Similarly, in 2009, a Michigan corporation was subject to a phishing scheme that resulted in $560,000 in unauthorized wire transfers from its bank account.[3] And in April 2011, the Federal Bureau of Investigation (FBI) issued an alert about the growing number of unauthorized wire transfers to China, in which small and medium-sized businesses suffered total losses of $11 million in 20 separate incidents.[4] This problem is also reflected in the increased number of Suspicious Activity Reports filed by financial institutions for "account takeovers," in which an unauthorized person takes control of a customer's account.[5]

These headlines undermine the public's confidence in the payment system. They also raise a critical question for banks and their business[6] customers: When funds are stolen from a bank account of a business customer through an unauthorized payment order, who bears the loss? For unauthorized wire transfers and ACH credit transfers, Article 4A of the Uniform Commercial Code (UCC) provides the legal framework for determining who is responsible for any resulting losses.[7] This article examines the relevant provisions of Article 4A, reviews two recent federal appeals court decisions interpreting these provisions in the context of funds stolen through unauthorized wire transfers and ACH credit transfers, and discusses sound practices to mitigate this risk in light of the UCC's requirements and these court cases.

---

[1] Association for Financial Professionals, *2015 AFP Payments Fraud and Control Survey: Report of Survey Results*, 2015. Bethesda, MD: Association for Financial Professionals, available at http://ow.ly/MIraf.

[2] See Brian Krebs, "$1.66M in Limbo After FBI Seizes Funds from Cyberheist," *Krebs on Security*, September 14, 2014, available at http://krebsonsecurity.com/tag/luna-luna-llp/. Actually, $1.75 million in transfers were made, and the bank was able to recover $89,651, leaving a net loss of $1.66 million. The bank is currently in litigation with the law firm over responsibility for the losses. *Texas Brand Bank v. Luna & Luna, LLP* (Case No. 3:14-1134, N.D. Tex. 2014), available at http://ow.ly/NTVqy.

[3] See *Experi-Metal, Inc. v. Comerica Bank*, 2011 WL 2433383 (E.D.Mich. 2011), available at http://ow.ly/MRdsC. The initial amount of unauthorized wire transfers was $1,901,269, but the bank was able to reverse some of the transfers.

[4] FBI, Financial Services Information Sharing and Analysis Center, and Internet Crime Complaint Center, "Fraud Alert Involving Unauthorized Wire Transfers to China," April 26, 2011, available at www.ic3.gov/media/2011/chinawiretransferfraudalert.pdf.

[5] Suspicious Activity Reports for account takeovers are discussed in the U.S. Department of the Treasury, Financial Crimes Enforcement Network, "Account Takeover Activity," Advisory FIN-2011-A016, December 19, 2011, available at http://ow.ly/MIyUU. Additional information on the incidence of payment fraud is available on the website of the Association for Financial Professionals, which publishes an annual survey of its members, at www.afponline.org/fraud/.

[6] For consumer bank accounts, the Electronic Fund Transfer Act (EFTA), as implemented by Regulation E, determines who is responsible for unauthorized transactions. See 15 U.S.C. 1693g, available at http://ow.ly/MQDXX, and 12 CFR 1005.6, available at http://ow.ly/MQE9N.

[7] Article 4A does not apply to an ACH debit transfer, which is initiated by the person receiving the transfer instead of the person sending it. See Official Comment 4 to UCC section 4A-104, available at http://ow.ly/MQG4s. ACH debit transfers are governed by the rules of the National Automated Clearing House Association. *Keppler v. RBS Citizens N.A.*, 2014 WL 2892352 (D.Mass. 2014) (discussing different rules that apply to ACH credit transfers and debit transfers).

Impact on Community Banks

Account takeovers are an important issue for community banks because criminals are increasingly targeting small and mid-sized companies, which are believed to have less-sophisticated security systems than larger companies.[8] These companies, in turn, often bank with community banks.[9] According to Symantec, the software security firm, 50 percent of all "spear-phishing" attacks (in which the criminal sends an e-mail with a malware attachment or malicious links that appears to be from an individual or business known to the recipient) targeted businesses with 2,500 or fewer employees in 2011, and by 2013, this number had increased to 61 percent of all attacks.[10] By infiltrating a business's computer system, the criminal can obtain the log-in credentials to the business bank accounts and initiate unauthorized payment orders. Thus, it is important for community banks to understand the requirements of Article 4A of the UCC that come into play when a dispute arises between a bank and its business customers because of unauthorized wire transfers or ACH credit transfers, as well as ways to address the risks arising from unauthorized transfers.

UCC Article 4A

By default, Section 4A-204(a) provides that a bank is responsible for any unauthorized electronic payment orders on a nonconsumer account. However, Section 4A-202(b) permits a bank to shift the risk of loss to its customers if it follows these procedures:

- The bank and its customer agree that the bank will authenticate any payment orders on the account under an agreed-upon security procedure.
- The security procedure is "commercially reasonable."
- The bank complied with the procedure, acted in good faith, and implemented the customer's written instructions (if any) restricting payment.

Because these requirements focus heavily on a bank's use of a "commercially reasonable" security procedure, the definition of this term is critical. Article 4A provides two ways for a bank to establish that its security procedure is commercially reasonable. First, under Section 4A–202(c), a bank can show that its procedure took into account:

- the wishes of the customer expressed to the bank;
- the circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank;
- alternative security procedures offered to the customer; and
- the procedures in general use by customers and receiving banks similarly situated.[11]

The UCC includes Official Comments for clarification. According to Comment 4 for Section 4A–202(c), which is referenced in Section 4A-203, the meaning of "commercially reasonable" is flexible and depends on the particular circumstances of the bank and its customer. For example, a customer transmitting a large number of high-dollar payment orders may reasonably expect state-of-the-art security procedures, while a customer with a small number of transactions or low-dollar amount transactions may have different expectations. Similarly, "it is reasonable to require large money center banks to make available state-of-the-art security procedures. On the other hand, the same requirement may not be reasonable for a small country bank."[12] The comment also

continued on page 14

"Account takeovers are an important issue for community banks because criminals are increasingly targeting small and mid-sized companies, which are believed to have less-sophisticated security systems than larger companies."

[8] Geoffrey Fowler and Ben Worthen, "Hackers Shift Attacks to Small Firms," *Wall Street Journal*, July 21, 2011.

[9] Allen N. Berger, William Goulding, and Tara Rice, "Do Small Businesses Still Prefer Community Banks?" Board of Governors of the Federal Reserve System, International Finance Discussion Papers 1096, December 2013, available at www.federalreserve.gov/pubs/ifdp/2013/1096/ifdp1096.pdf.

[10] Symantec Corporation, *Internet Security Threat Report 2014*, vol. 19, April 2014, available at http://ow.ly/MRfQO.

[11] These requirements appear in UCC Section 4A–202(c).

[12] Official Comment 4 to UCC Section 4A-203.

What Explains Low Net Interest Income at Community Banks?

by Charles S. Morris, Vice President and Economist, Federal Reserve Bank of Kansas City and Kristen Regehr, Assistant Economist, Federal Reserve Bank of Kansas City

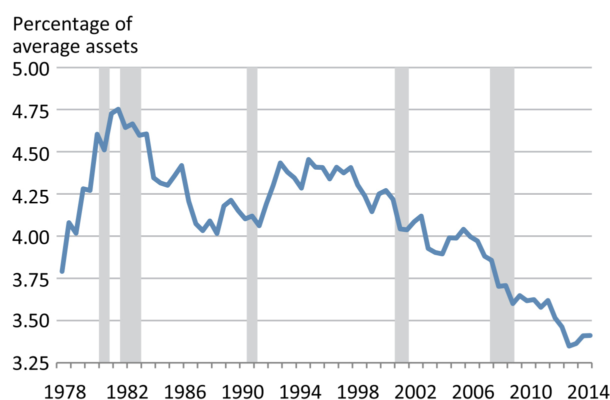
Community bank profitability declined sharply during the 2007–09 financial crisis and recession. Profitability has improved since the crisis, primarily due to declines in loan-loss provisions. Net interest income — the largest source of revenue for community banks — has remained flat, however, and is below precrisis levels. According to many observers, including community bankers, the low interest rate environment has made it difficult for financial institutions to earn an adequate spread on loans since the recession ended. In addition, bankers say weak lending opportunities and loan demand have contributed to reduced interest income.

This article summarizes the findings of a recent study that discusses the factors that most influence community bank net interest income and the extent to which these factors are contributing to the current low levels of net interest income.[1] Additionally, the article examines whether net interest income (since the crisis and recession began) is abnormal relative to historical experience. The results of the study suggest the lack of recovery in community bank net interest income seven years after the start of the financial crisis and recession is not unusual given economic and banking conditions.

Historical Background

Community bank[2] net interest income has varied significantly over the past 38 years. In order to compare how net interest income performed during the most recent recovery relative to previous recoveries, we conducted an analysis of net interest income starting in 1977. The 1973–75 and 1981–82 recessions, along with the 2007–09 recession, were the three longest recessions since the Great Depression. Figure 1 shows the average net interest income over the study period. During the study period, average net interest income for community banks varied from a high of 4.75 percent of average assets in the first half of 1981 to a low of 3.35 percent in the first half of 2013. Net interest income for the second half of 2014 was 3.41 percent.[3]

Figure 1: Community Bank Net Interest Income: Historical Perspective



Source: Consolidated Reports of Condition and Income
Notes: Sample net interest income (semiannual) annualized as a percentage of average assets over the previous year. The shaded bars depict recession quarters. See Morris and Regehr (2014).

What Banking and Economic Factors Affect Net Interest Income?

Given the variability of net interest income, it is not surprising that the banking and economic factors expected to most affect net interest income also varied significantly over this period. From 1977 to 2014, there were large variations, as measured by standard deviations, in the 1-year U.S. Treasury bill rate, the average loan-to-asset ratio, and the average nonmaturity deposit-to-liability ratio (Table 1). Understanding how these factors *should* affect net interest income is important for understanding if the results from a model that *estimates* their effects make sense.

---

[1] See Charles S. Morris and Kristen Regehr, "What Explains Low Net Interest Income at Community Banks?" *Economic Review*, Federal Reserve Bank of Kansas City, 2014 Second Quarter, at www.kansascityfed.org/~/media/files/publicat/econrev/econrevarchive/2014/2q14morris-regehr.pdf for a description of the data.

[2] While the Federal Reserve typically defines community banks as those with $10 billion or less in total assets, for the purpose of this analysis, community banks are defined as banks with total assets of $1 billion or less in 2012 dollars.

[3] The data are semiannual instead of quarterly because the income portion of the Consolidated Reports of Condition and Income (commonly known as the Call Report) was filed only semiannually prior to 1983.

Table 1: Variability of Factors Affecting Net Interest Income (1976H1–2014H2)

Factors	Maximum	Minimum	Range	Standard Deviation
Net Interest Income	4.75	3.35	1.40	0.34
1-Year U.S. Treasury Rate	14.93	0.11	14.82	3.73
Spread (10-Year–1-Year U.S. Treasury Rate)	3.23	-1.43	4.66	1.15
Loan-to-Asset Ratio	66	50	16	4.7
Nonmaturity Deposit-to-Total Liability Ratio	64	40	24	4.9

Source: Consolidated Reports of Condition and Income
Note: See Morris and Regehr (2014) for a description of the data.

Changes in market interest rates — both the absolute and relative levels — have perhaps the most significant effect on net interest income in the short term. When interest rates change, the degree to which net interest income changes depends on a bank's asset and liability maturity structure and the extent to which a bank's loan and deposit rates reset when market rates change prior to maturity. A bank is said to be asset sensitive if its assets have a shorter maturity or reprice faster than liabilities and is liability sensitive when the converse is true.[4] These relative sensitivities imply that a parallel increase in the yield curve increases net interest income for asset-sensitive banks and decreases net interest income for liability-sensitive banks. These relationships are shown in the first (1) column of Table 2.

[4] The repricing effects here include the total effects that account for factors such as floors on loan rates and the historical "stickiness" of deposit rates when interest rates rise.

Table 2: Effect of Changes in the Level and Slope of the Yield Curve on Net Interest Income

	Parallel Increase in Yield Curve (1)	Change in Slope of Yield Curve Due to Change in One Rate Holding the Other Constant:	
		Increase in Long-Term Rates (steeper) (2)	Increase in Short-Term Rates (less steep) (3)
Asset-Sensitive	↑	↑	↑
Liability-Sensitive	↓	↑	↓

The effects of changes in the slope of the yield curve on net interest income not only depend on whether a bank is asset or liability sensitive but also on whether the change in the slope is due to a change in long-term or short-term interest rates, as shown in the second (2) and third (3) columns of Table 2. If long-term rates increase so that the yield curve is steeper, net interest income will increase regardless of whether banks are asset or liability sensitive. This is because higher long-term rates affect only new and maturing long-term loans and investments, both of which will earn higher returns and can be funded with short-term liabilities at unchanged rates.

However, when short-term rates increase, which decreases the slope of the yield curve, the effect on net interest income depends on whether the bank is asset or liability sensitive. For an asset-sensitive bank, a rise in short-term rates will cause net interest income to increase because the interest income from new short-term assets and current assets that reprice off short-term rates will rise more than the interest expense on short-term deposits. In contrast, for a liability-sensitive bank, an increase in short-term rates will decrease net interest income because the interest expense on short-term deposits will rise more than the interest income on new short-term and current repricing assets.

Net interest income is also affected by the composition of assets and liabilities. Among a bank's assets, loans generally have a higher interest rate than marketable securities do because loans tend to be riskier. Among liabilities, nonmaturity deposits tend to have the lowest interest expense, partly because a large share of nonmaturity deposits generally pay lower interest rates than comparable deposits that do not provide transactions services. As a result, net interest income should increase as the loan-to-asset or nonmaturity deposit-to-liability ratios increase.

What Does Regression Analysis Tell Us About Why Net Interest Income Is So Low?

To determine why net interest income has not recovered in the six years since the end of the financial crisis and recession, a "base" regression model is constructed to estimate the influence of various economic and banking variables on net interest income. Variables used in the model include market interest rates (1- and 10-year U.S. Treasury rates), bank balance sheet items (loan-to-asset and nonmaturity deposit-to-liability ratios and inflation-adjusted total assets), and macroeconomic conditions (real GDP growth and inflation).

continued on page 18

Some Thoughts on Community Banking: A Conversation with Chair Janet Yellen *continued from page 1*

tors than larger banks when making lending decisions, and they may also be willing to underwrite loans to creditworthy customers that large banking organizations may be unwilling to make. When you consider that there were more than 5,500 community banks in the United States as of year-end 2014, you can appreciate their collective reach and the important role that they play in the economy.

Q What are the common characteristics of community banks that failed as opposed to those that managed to thrive throughout the crisis?

A When I was the president of the Federal Reserve Bank of San Francisco, I saw firsthand the strain that the financial crisis had on community banks, and I observed that many bank failures could be traced to a bank's risk management practices not keeping pace with the expansion of its real estate lending activity. Many community banks that failed had high concentrations in commercial real estate, especially construction and development lending in markets that experienced significant decreases in real estate values. These concentrations became especially problematic at banks that did not have sufficient capital to absorb losses.

On the other hand, banks that managed to thrive throughout the crisis had what I consider to be a traditional business model — in other words, local deposit-taking and conservative lending — along with strong corporate governance, robust risk management frameworks, careful growth plans, and strategies that supported a reasonably well-diversified balance sheet. Concentrations of any type of loans add risk and require strong risk management. Even with strong risk management in place, however, healthy banks were not immune from losses; banks that had capital positions commensurate with their risk exposures were better able to absorb these losses and continue serving customers throughout the crisis.

Q What are some of the heightened risks that community banks are currently facing?

A Although community banks provide a wide range of services for their customers, their primary activities revolve around deposit-taking and lending. Risks at community banks primarily arise from their lending activity, in the form of credit risk, interest rate risk, or concentration risk, rather than from the types of trading, market-making, and investment banking activities associated with the largest banks.

While credit risk concentrations have historically contributed to problems at community banks, interest rate risk is also something that we are working with community banks to monitor. Our examiners have been reviewing whether banks are able to manage risks arising from future changes in rates. Fortunately, our sense so far has been that the vast majority of community banks are paying adequate attention to interest rate risk management, although we will of course be keeping a close eye on this risk going forward.

Another growing risk facing banks of all sizes is cybersecurity. Banks have not only suffered direct financial losses from cyberattacks, but they also must absorb costs associated with customer data breaches. As community banks are expanding their online banking services to meet customer needs and compete with large banking organizations, community banks need to stay informed of cyberthreats and implement strong controls to protect their operations against these attacks.

In response to the increasing frequency and sophistication of cyberattacks against banks, the Federal Financial Institutions Examination Council (FFIEC) in June 2013 created the Cybersecurity and Critical Infrastructure Working Group to address policies related to cybersecurity and critical infrastructure security.[2] We, along with our colleagues at the other FFIEC agencies, are devoting considerable resources to address cyber-related issues. In addition, we continually communicate and coordinate with the law enforcement and intelligence communities, as well as financial industry associations, on cybersecurity matters.

Federal Reserve Efforts to Solicit the Views of Community Banks

Q How does the Federal Reserve solicit the views of community bankers?

[2] See www.ffiec.gov/cybersecurity.htm.

A I consider it very important for the Federal Reserve to pay close attention to the issues and concerns facing community banks. That's why we have so many different ways to engage with and hear from community bankers. The leadership and staff at the 12 Federal Reserve Banks are in regular contact with community bankers in their districts. While I and my colleagues on the Board of Governors always appreciate the opportunity to travel to different parts of the country, the Reserve Banks in many ways serve as our eyes and ears, not only regarding supervisory issues, but also local economic trends. Reserve Banks host forums and other events throughout the year to meet with bankers to get their perspectives on banking issues, and Reserve Bank staff often share what they hear at these events with Board staff in Washington, D.C. In addition, I and other Board members meet regularly with community bankers.

We also have more formal mechanisms for hearing the views of bankers. For instance, the Federal Reserve formed the Community Depository Institutions Advisory Council (CDIAC) in 2010 to provide input to the Board of Governors on the economy, lending conditions, and other issues of interest to community depository institutions.[3] Representatives from banks, thrift institutions, and credit unions are selected to serve on local advisory councils at each of the Federal Reserve Banks. One member from each of the Reserve Bank councils is selected to serve on the national CDIAC, which meets twice a year with the Board of Governors in Washington, D.C., to discuss topics of interest to community depository institutions. I find these meetings to be interesting and informative.

In addition to the efforts already discussed, the Federal Reserve always welcomes the views of community bankers on proposed regulations issued for comment in the *Federal Register*. Comments from community bankers help us to scale rules and policies to appropriately reflect the risks at smaller institutions and to assess implementation complexity and cost.

Q Could you please describe the Economic Growth and Regulatory Paperwork Reduction Act (EGRPRA) review process?

A In accordance with the EGRPRA, the Federal Reserve, the other federal bank regulatory agencies,[4] and the FFIEC have launched a review to identify banking regulations that are outdated, unnecessary, or unduly burdensome. The agencies recently expanded the review to include regulations that are relatively new, including rules adopted or proposed in the implementation of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act).[5] We have issued three *Federal Register* notices seeking comments on our regulations thus far,[6] and we will publish one additional *Federal Register* notice over the next year. The agencies will submit a report to Congress that summarizes any significant issues raised by the comments and the relative merits of such issues.

The agencies also have begun a series of outreach meetings with bankers, consumer groups, and other interested parties to discuss the review.[7] Community bankers are encouraged to express their views on the regulations under review in a comment letter or at one of the outreach meetings.

Schedule of EGRPRA Outreach Meetings

Locations	Dates
Los Angeles	December 2, 2014[a]
Dallas	February 4, 2015[a]
Boston	May 4, 2015[a]
Kansas City[b]	August 4, 2015
Chicago	October 19, 2015
Washington, D.C.	December 2, 2015

[a] Although these meetings have already taken place, agendas, videos, and transcripts are available at http://ow.ly/ODJu7.
[b] The outreach meeting to be held in Kansas City will focus more specifically on issues affecting rural institutions.

I can certainly say, though, that the comments from the industry, consumer groups, and others have been very informa-

[3] See federalreserve.gov/aboutthefed/cdiac.htm.

[4] The other federal bank regulatory agencies are the Federal Deposit Insurance Corporation (FDIC) and the Office of the Comptroller of the Currency (OCC).

[5] The review encompasses consumer regulations that were not transferred to the Consumer Financial Protection Bureau but remained with the banking agencies.

[6] Board of Governors of the Federal Reserve System, FDIC, and OCC, "Federal Bank Regulatory Agencies Seek Comment on Interagency Effort to Reduce Regulatory Burden," press releases, June 4, 2014, February 20, 2015, and May 29, 2015, available at www.federalreserve.gov/newsevents/press/bcreg/20140604a.htm, www.federalreserve.gov/newsevents/press/bcreg/20150220a.htm, and www.federalreserve.gov/newsevents/press/other/20150529b.htm, respectively.

[7] See the FFIEC's EGRPRA website at http://egrpra.ffiec.gov/ for more information.

tive and will help us and our colleagues at the other agencies to assess regulatory burden. We have received comments on a variety of issues, and I expect we will receive many more comments in the coming months. Since we are only midway through the EGRPRA process, it is too soon to form any definitive conclusions, but several themes have arisen so far in the process.

One recurring theme in the comments has been the question of whether the agencies could reevaluate regulations that may constrain the lending activities of community banks. For example, community bankers have asked the agencies to consider increasing the dollar threshold in their appraisal regulations for transactions below which an appraisal would not be required. This change may provide relief to community bankers by allowing them to use a less-formal valuation of collateral for a larger number of loans, especially in rural areas where it can be difficult to find an appraiser with knowledge about the local market at a reasonable fee.

A number of community banks have also suggested reducing the burden from required quarterly reporting of the Consolidated Reports of Condition and Income (commonly called the Call Report). Working through the FFIEC, the Federal Reserve is considering ways we could perhaps respond to industry concerns about Call Report filing requirements and assessing the potential impact of collecting less data from banks.

The agencies will consider all the feedback gathered at these meetings and in written comments in the ongoing assessment of our regulations. In some cases, legislative action to update the federal statutes upon which the agencies base our regulations may be needed to implement the suggested changes.

Federal Reserve Efforts to Address Community Bankers' Concerns

Q What steps have been taken by the Federal Reserve to address concerns raised by community bankers about the burden of new regulations and supervisory requirements?

A Community bankers often raise concerns about the time demands of the examination process and the higher expenses that can arise from new supervisory regulations and policies. In that regard, we are taking steps to tailor and improve our examination processes to be more efficient for lower-risk banks. For example, some aspects of the loan review process can be conducted offsite for banks that maintain certain electronic loan records. This reduces the burden on many community banks and often reduces the time spent onsite by Federal Reserve examiners.

With respect to supervisory regulations and policies, we recognize that the cost of compliance can have a disproportionate impact on smaller banks, as they have fewer staff members available to help comply with additional regulations. To address this, we work within the requirements of the law to draft rules that are not unduly burdensome for community banks to implement. This is evident in many of the Federal Reserve regulations implementing the Dodd-Frank Act, where the most stringent requirements apply only to the largest and most complex banking organizations and not to community banks.

The Board also relies on its Subcommittee on Smaller Regional and Community Banking of the Committee on Bank Supervision to review proposed supervisory policies and weigh the potential effect on community banks.[8] This subcommittee oversees the supervision of community and regional banks and reviews proposed supervisory policies to help ensure that they are appropriate for, and tailored to, community banks.

As we develop supervisory policies and examination practices, we are very mindful of community bankers' concerns that new requirements for large banking organizations could inadvertently be viewed as "best practices" for the financial sector that trickle down to community banks in a way that is inappropriate for the risks that they face. To address this concern, we have been enhancing our communications with and training for examination staff about expectations for community banks versus large banking organizations to ensure that expectations are calibrated appropriately. When our examiners are trained effectively and kept informed of newly issued policies in a timely manner, they are better equipped to understand the supervisory goals of regulations and guidance and to provide appropriate feedback to bankers.

Q Can you share any examples of how the Federal Reserve has modified supervisory policy to provide regulatory relief to community banks?

A In April of this year, the Federal Reserve Board approved a final rule that increased the asset threshold of its Small Bank Holding Company Policy Statement from $500 million to $1 billion and applied the policy statement to savings and loan holding companies.[9] The policy statement facilitates the

[8] See www.federalreserve.gov/aboutthefed/bios/board/default.htm.

transfer of ownership of small community banks and savings associations by allowing their holding companies to operate with higher levels of debt than would normally be permitted. Holding companies that qualify for the policy statement are also excluded from consolidated capital requirements, though their depository institution subsidiaries continue to be subject to minimum capital requirements. All qualifying firms must still meet certain qualitative requirements, including those pertaining to nonbanking activities, off-balance sheet activities, and publicly registered debt and equity.

Concurrently, the Board reduced the regulatory reporting burden for bank holding companies and savings and loan holding companies with less than $1 billion in total consolidated assets that meet the qualitative requirements of the policy statement.[10] Before we made this change, companies subject to the policy statement reported 65 pages of data items; they now need to report only eight pages of data items.

[9] See www.federalreserve.gov/newsevents/press/bcreg/20150409a.htm.

[10] Specifically, the Board eliminated quarterly and more complex consolidated financial reporting requirements for these institutions (FR Y-9C) and instead now requires parent-only financial statements (FR Y-9SP) semiannually.

Federal Reserve Resources Available to Community Banks

Q What tools does the Federal Reserve provide to assist community banks?

A In addition to this publication, the Federal Reserve offers various free resources to community bankers, including online training for bank directors and conference calls in which Federal Reserve staff members speak with bankers on current banking issues. I encourage community bankers to discuss their questions with their local Reserve Bank and, if they have issues or concerns, to work with our staff to try to resolve these issues before the examination review process begins. Ongoing dialogue between the Federal Reserve and community banking institutions is quite important. And I welcome hearing from community bankers from across the country, since I believe we share the common goal of a safe and sound banking system and a strong economy. ■

Community Bank Resources

Ask the Fed consists of periodic conference calls for bankers that feature Federal Reserve experts and guest speakers discussing top banking issues, with time at the end for questions and comments. For further information, visit www.askthefed.org.

Basics for Bank Directors, now in its fifth edition, is a reference guide for bank directors. This publication details the processes and procedures for promoting the stability, growth, and success of banks. For more information, visit www.kansascityfed.org/Publicat/BasicsforBankDirectors/BasicsforBankDirectors.pdf.

Bank Director's Desktop provides online training for bank directors that introduces corporate governance and director duties and responsibilities; covers basic bank financial analysis; and discusses the sources, control, and monitoring of portfolio risks, including credit, liquidity, and market risks. For more information, visit www.bankdirectorsdesktop.org/.

Community Banking Connections is a quarterly publication, available in print and online, dedicated to addressing issues that community banks currently face, providing resources on key supervisory policies, highlighting new regulations, and offering perspectives from bank examiners and other Federal Reserve staff. For more information, visit www.cbcfrs.org.

Consumer Compliance Outlook is a quarterly Federal Reserve System publication dedicated to consumer compliance issues. For further information, visit www.consumercomplianceoutlook.org/.

FedLinks consists of a series of single-topic bulletins prepared specifically for community bankers that highlight key elements of a supervisory topic to improve clarity and understanding about the topic and examiner expectations for applying related supervisory guidance. For further information, visit www.cbcfrs.org/fedlinks.

Outlook Live is a popular webinar series that delves deeper into consumer compliance topics of interest. For further information, visit www.consumercomplianceoutlook.org/outlook-live/.

Partnership for Progress is a national outreach effort to help minority-owned institutions confront unique business model challenges; cultivate safe banking practices; and compete more effectively in the marketplace through a combination of one-on-one guidance, workshops, and an extensive interactive web-based resource and information center. For more information, visit www.fedpartnership.gov/.

What Community Bankers Should Know About Virtual Currencies *continued from page 3*

Reputational Risk

Another important risk for community banks to consider is reputational risk. The February 2014 failure of Mt. Gox, the largest Bitcoin exchange and wallet provider at the time, illustrates how a bank's reputation can be damaged because of the activities of its customers. In this case, Mt. Gox failed after losing more than $400 million of its customers' bitcoins. Clearly, Mt. Gox did not have sufficient controls in place to ensure the bitcoins were secure. Since then, multiple lawsuits have been filed against Mt. Gox, with several also naming Mt. Gox's bank as a defendant. Although the bank never held the bitcoins, it did handle Mt. Gox's transactional banking needs. At least one of the lawsuits claims that the bank should have known about the fraud and that the bank profited from the fraud.

In addition to any impact to the bank's reputation resulting from its relationship with a failed virtual currency firm, there is also the potential legal and financial impact if the bank settles or loses any of these lawsuits.

Credit Risk

How should a community bank respond if a borrower wants to specifically post bitcoins or another virtual currency as collateral for a loan? For many, virtual currencies are simply another form of cash, so it is not hard to imagine that bankers will face such a scenario at some point. In this case, caution is appropriate. Bankers should carefully weigh the pros and cons of extending any loan secured by bitcoins or other virtual currencies (in whole or in part), or where the source of loan repayment is in some way dependent on the virtual currency. For one, the value of a bitcoin in particular has been volatile. The figure at right shows the dollar value of one bitcoin from November 25, 2013, to January 25, 2015. Thus, the collateral value could fluctuate widely from day to day. Bankers also need to think about control over the account. How does a banker control access to a virtual wallet, and how can it limit or control the borrower's access to the virtual wallet? In the event of a loan default, the bank would need to take control of the virtual currency. This will require access to the borrower's virtual wallet and private key. All of this suggests that the loan agreement needs to be carefully crafted and that additional steps need to be taken to ensure the bank has a perfected lien on the virtual currency.

Figure: Bitcoin Price Index Chart

Source: www.coindesk.com

Operational Risk

What if the bank actually owns the virtual currency? For example, it is possible a bank could find itself acquiring virtual currency in satisfaction of debts previously contracted. The most likely scenario in which this could occur is when a bank makes a business loan secured by the borrower's business assets, which at default include virtual currency. At the moment, such a scenario is unlikely, but its plausibility increases as virtual currency becomes more mainstream.

Holding virtual currency presents some operational challenges for a financial institution. The virtual currency acquired in this manner should certainly be liquidated in an orderly fashion, but before that happens, the institution will need to have internal controls in place to mitigate the risk of loss. Management should establish dual control and access processes, as well as think about how this asset will be valued and accounted for on its financial statements. Management will also have to consider the security of the virtual currency itself, how it is held, and how vulnerable it is to theft.

Conclusion

Virtual currencies bring with them both opportunities and challenges, and they are likely here to stay. Although it is still too early to determine just how prevalent they will be in the coming years, we do expect that the various participants in the virtual currency ecosystem will increasingly intersect with the banking industry. Banks need not turn away this business as a class, but they should consider the risks of each individual customer. This will require bank management to broadly understand all the risks involved with conducting banking with these businesses. However, the risk will vary significantly depending on the specific nature of the business, and in many cases, bank management teams may correctly determine that the risk is no more significant than the risk presented by any other customer. In other situations though, the risk may be heightened and require additional due diligence, ongoing monitoring, or establishment of additional controls to appropriately manage and control the risk. ■

Additional Resources

The Federal Reserve's Ask the Fed program is an excellent resource for additional information about virtual currencies. In July 2014, the Fed held two sessions on Bitcoin Payments. These sessions focused on the transactional process of virtual currencies and included a discussion of exchanges, mining, wallets, and storage. The second set of sessions, held on September 17 and November 10, 2014, focused solely on BSA/AML compliance issues related to virtual currency. Community bankers can register to access the archived versions of these presentations by visiting www.askthefed.org.

REGULATORY RECAP

Supervision & Regulation (SR) & Consumer Affairs (CA) Letters

The following SR and CA letters that have been published since the last issue (and are listed by most current) apply to community banking organizations. Letters that contain confidential supervisory information are not included. All SR letters are available by year at www.federalreserve.gov/bankinforeg/srletters/srletters.htm and by topic at www.federalreserve.gov/bankinforeg/topics/topics.htm. A complete list of CA letters can be found at www.federalreserve.gov/bankinforeg/caletters/caletters.htm.

SR Letter 15-9, "FFIEC Cybersecurity Assessment Tool for Chief Executive Officers and Boards of Directors"

SR Letter 15-8, "Name Check Process for Domestic and International Applications"

SR Letter 15-6, "Interagency Frequently Asked Questions (FAQs) on the Regulatory Capital Rule"

CA Letter 15-4, "Expiration of the Protecting Tenants at Foreclosure Act"

CA Letter 15-3, "Revised Interagency Examination Procedures for Regulation Z and Regulation X"

Managing the Risk of Unauthorized Payments from Business Bank Accounts continued from page 5

notes that the "standard is not whether the security procedure is the best available. Rather it is whether the procedure is reasonable for the particular customer and the particular bank, which is a lower standard. On the other hand, a security procedure that fails to meet prevailing standards of good banking practice applicable to the particular bank should not be held to be commercially reasonable."

The second way to establish that a procedure is commercially reasonable applies when a customer declines a security procedure offered by a bank because the customer wants to use its own security procedure. If the customer agrees in writing to be bound by any payment order, whether or not authorized, that is issued in its name and accepted by the bank that complies with the customer's chosen security procedure, the procedure is deemed commercially reasonable, provided that the procedure offered by the bank that the customer declined satisfied the commercially reasonable requirements set forth previously.[13]

Recent Court Cases Interpreting Commercially Reasonable Security Procedures

Two recent federal appellate court decisions examined different aspects of Article 4A's requirements and help to clarify the steps financial institutions must undertake to avoid responsibility for losses incurred by their customers.[14]

Case One: Bank's Security Procedure Is Not Commercially Reasonable

In *Patco Construction Co. v. People's United Bank*,[15] unauthorized ACH credit transfers totaling $588,851 were taken from PATCO Construction Company's account with Ocean Bank, a mid-sized bank later acquired by People's United Bank. PATCO was able to recover $243,406, leaving a net loss of $345,444. PATCO sued the bank to recover its loss. The crucial issue on appeal was whether the bank's security system was commercially reasonable as defined in the UCC.

The court found flaws in the way the bank implemented its security system. First, if a transaction exceeded a specified threshold, the customer had to answer challenge response questions (for example, "What is your mother's maiden name?"). The bank set the threshold at one dollar or more for all of its customers. The court found the one-dollar threshold meant that *every* transfer would trigger challenge response questions. If a customer's computers were infected with key-logging malware, which records a computer user's keystrokes and transmits the information over the Internet, the risk of malware recording the answers to the challenge questions increased substantially because every transaction — which for PATCO included all payroll transfers — triggered a challenge response.

Second, the bank failed to monitor the warnings from its security software. The software generated a score for every ACH transaction based on certain risk factors. The security system flagged the unauthorized transactions as very high risk. However, because the bank did not monitor the risk scores, it did not notify PATCO or try to stop the transactions pending verification.

Finally, the court noted that key-logging malware was an industry concern when the transactions occurred and that many Internet banking security systems were using hardware tokens as an additional security measure, which the Federal Financial Institutions Examination Council (FFIEC) had recommended as a useful part of a multifactor authentication scheme.[16] Other banks performed manual reviews or custom-

[13] UCC Section 4A–202(c).

[14] Decisions of federal appeals courts are binding on the federal courts in their jurisdiction. The First Circuit encompasses Massachusetts, Maine, New Hampshire, Rhode Island, and Puerto Rico, whereas the Eighth Circuit encompasses Arkansas, Iowa, Minnesota, Missouri, Nebraska, North Dakota, and South Dakota. For banks operating in other states, these decisions are persuasive but not binding authority.

[15] *Patco Construction Co. v. People's United Bank*, 684 F.3d 197 (1st Cir. 2012), available at http://ow.ly/MQNCG.

[16] FFIEC, "Authentication in an Internet Banking Environment," 2005, available at http://www.ffiec.gov/pdf/authentication_guidance.pdf. In 2011, the FFIEC published supplemental authentication guidance to update the member agencies' expectations "regarding customer authentication, layered security, or other controls in the increasingly hostile online environment."

er verification for high-risk transactions. Ocean Bank did not use any of these security measures and thus was not complying with the UCC requirement to consider the security procedures used by customers and at similarly situated banks.

In light of these problems, the First Circuit concluded that Ocean Bank's security procedures were not commercially reasonable. However, the court noted that PATCO also had responsibilities for implementing security procedures, so the court sent the case back to the trial judge to determine if PATCO bore any responsibility for the unauthorized transactions. But after the First Circuit issued its opinion, the bank settled the case for the amount of the loss ($345,444) plus interest.[17]

Case Two: Bank's Security Procedure Is Commercially Reasonable

The second case, *Choice Escrow & Land Title, LLC v. BancorpSouth Bank*,[18] concerned the responsibility between BancorpSouth Bank and its business customer, Choice Escrow & Land Title, for $440,000 in unauthorized ACH transactions. An employee at Choice clicked on a link in a phishing e-mail that allowed malware to be installed on a network computer. As a result, hackers were able to issue a fraudulent payment order for $440,000 that was sent to a foreign country. Choice sued the bank to recover the $440,000.

The bank's security system offered four security features: (1) user ID and password requirement; (2) registration of an authorized user's Internet protocol (IP) address and computer information when the user first registered; (3) the customer's ability to place dollar limits on transactions; and (4) dual control, which required that every payment order request by an authorized user be approved by a second authorized user. If a customer declined the dual-control feature, the bank had the customer sign a waiver acknowledging it understood the risks of a single-control security system.

Choice declined the dollar limit on transactions and the dual-control feature and signed the waiver. Thus, the security procedure for Choice's ACH transactions consisted of a user ID and password and verification of IP address and computer information. Choice had also asked the bank whether its system had the capability to limit ACH transfers to foreign banks because of a concern about phishing scams. The bank responded that it was not possible, but that Choice could mitigate the risk of unauthorized ACH transactions if it implemented dual control, which Choice declined.

The court reviewed the bank's security procedure and determined it was commercially reasonable. For the requirement that a security procedure must be one in general use by similarly situated customer and banks, the court focused on the FFIEC's 2005 guidance. The guidance states that most modern authentication is multifactor and that "single-factor authentication, as the only control mechanism, [is] inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties."[19]

The court also noted that the FFIEC guidance states that threats change over time and that banks must "[a]djust, as appropriate, their information security program[s] in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information." The court noted the bank offered the dual-control option in response to increased security threats, which the court said was a reasonable response to the threat of phishing scams and thus was consistent with the FFIEC guidance.

The court next considered the requirement that a bank's security procedures must be suitable for the customer in light of "the wishes of the customer expressed to the bank" and "the circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank."[20]

Choice argued that the dual-control option failed to take into account Choice's circumstances because dual-control verification of every wire transfer was not feasible for Choice because of its small staff. But the court found that dual control was feasible for Choice: Choice's ACH transfers usually did not require immediate processing, so if an ACH request was received on a day when the dual-control employee was unavailable, that employee could approve it the next day without adverse consequence. When Choice declined the dual-control option, the court noted that it assumed the risks of this decision under the UCC, which states that when "an

[17] Tracy Kitten, "PATCO Settlement: What It Means," *Bank Info Security*, December 24, 2012, available at http://ow.ly/MQQ9U.

[18] *Choice Escrow & Land Title, LLC v. BancorpSouth Bank*, 754 F.3d 611 (8th Cir. 2014).

[19] FFIEC guidance, p. 4.

[20] Section 4A-202(c).

informed customer refuses a security procedure that is commercially reasonable and suitable for that customer and insists on using a higher-risk procedure because it is more convenient or cheaper," the customer assumes "the risk of failure of the procedure and cannot shift the loss to the bank."[21]

The court concluded that the bank's security procedures of password protection, daily transfer limits, device authentication, and dual control were commercially reasonable for the bank's customer.

Section 4A-202(b)(ii) imposes one final requirement for transferring liability to the customer: The bank must have "accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer." The court distilled this to mean that "the bank must abide by its [security] procedures in a way that reflects the parties' reasonable expectations as to how those procedures will operate."

The court noted that Choice was aware that when a payment order was approved through the agreed-upon security procedure, the bank employee's role was not to look for irregularities but to send the payment. The bank provided testimony that this was common practice in the industry. The bank thus satisfied the final requirement.

After considering this whole analysis, the Eighth Circuit upheld the lower court ruling that the bank's security procedure was commercially reasonable, and the bank was, therefore, not responsible for the unauthorized transactions.

Sound Practices in Light of *Patco* and *Choice*

These two cases help clarify the meaning of a commercially reasonable security procedure under the UCC for purposes of determining whether a bank or its commercial customer bears the risk of loss for unauthorized wire transfers and ACH credit transfers. Several themes that are relevant for community banks emerge from these opinions:

- **Understand and compare security procedures offered by different vendors and document the rationale for the procedure selected.** The UCC requires that a commercially reasonable security procedure be "in general use by customers and receiving banks similarly situated." The commentary also states that "a security procedure that fails to meet prevailing standards of good banking practice applicable to the particular bank should not be held to be commercially reasonable." Therefore, it is important for banks to discuss with security vendors the procedures other similarly situated banks are using for comparable customer situations. In *PATCO*, the court noted that Ocean Bank's peers were using tokens and one-time passwords, but Ocean Bank had not implemented either.
- **Use security procedures that meet the FFIEC guidelines.** Both the *PATCO* and *Choice* cases establish that compliance with the FFIEC guidelines, including supplements, is crucial because these guidelines are viewed by the courts as part of the industry security standard. The FFIEC guidelines state that "financial institutions should perform periodic risk assessments considering new and evolving threats to online accounts and adjust their customer authentication, layered security and other controls as appropriate in response to identified attacks." As a corollary, a bank is expected to monitor changes to the FFIEC guidance and respond accordingly. For example, the 2011 guidance states that financial institutions should adopt "layered security programs" that detect and respond to suspicious activity and include enhanced controls for system administrators, who have authority to change computer system configurations.
- **Have staff monitor and respond to security software notifications**. It is not enough to have security software that identifies risks; it is important that staff continuously monitor security alerts from the software and respond appropriately. In *PATCO*, the software identified high-risk transactions, but the bank was not monitoring this information when the security breaches occurred. The UCC commentary for Section 4A-203 confirms the importance of this by stating: "If the fraud was not detected because the bank's employee did not perform the acts required by the security procedure, the bank has not complied [with the security procedure]."
- **Be aware that security should not be "one-size-fits-all."** The security procedure should take into account "the circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank." A customer who makes five wire transfers of less than $5,000 per year, for example, requires a different security procedure than a customer making thousands of wire transfers every year, in large amounts, and to many foreign countries.

[21] Section 4A-203, Comment 4.

- **Proactively discuss security issues and best practices with customers.** Many unauthorized transaction cases occur when a bank customer's employee receives a phishing or malware e-mail that enables criminals to obtain log-in credentials to perform unauthorized transactions. In particular, spear phishing e-mails often target key employees who have access to accounts. Banks should be proactive with their customers to discuss ways to mitigate this risk. For example, a bank could recommend that the customer allow only electronic transfers to be performed on a dedicated computer that cannot access e-mail or the Internet, to reduce the risk of exposure to phishing, malware e-mails, and web pages with malware.[22] Banks could also encourage customers to conduct regular cybersecurity training to reduce the risk of an employee falling victim to a phishing or malware e-mail attack. Banks should also encourage their customers to use antiphishing software to help detect and protect against phishing e-mails.

Conclusion

Cybersecurity breaches are on the rise, and lawsuits seeking reimbursement for the resulting losses are rising, too. In the event of a legal dispute over responsibility for unauthorized wire transfers and ACH credit transfers for a business bank account, courts will look to Article 4A of the UCC to determine who bears the loss based primarily on whether a bank has implemented a commercially reasonable security procedure. The standard under the UCC is not whether the security procedure is the best available; rather it is whether the procedure is reasonable for the particular customer and the particular bank.

Of course, no bank wants to be in litigation with its customers. Thus, banks should proactively discuss with their business customers ways to appropriately identify, measure, monitor, and control cybersecurity risks, taking into account the particular risks and circumstances of the customer's operations. This will help banks to prevent unauthorized payments from occurring, reduce losses, retain satisfied customers, and increase public confidence in payment systems. ■

[22] For other examples of ways to mitigate cybersecurity risk, see the March 12, 2010, Cyber Security Advisory, "Information and Recommendations Regarding Unauthorized Wire Transfers Relating to Compromised Cyber Networks," of the National Council of Information Sharing and Analysis Centers at http://ow.ly/NTVK8. In addition, the Texas Bankers Electronic Crimes Task Force, working with other agencies, published "Best Practices: Reducing the Risks of Corporate Account Takeovers" in 2011, which is available at http://ow.ly/NTVMw.

FedLinks®
Connecting Policy with Practice

FedLinks: Connecting Policy with Practice is a single-topic bulletin prepared specifically for community banks and bank holding companies with total assets of $10 billion or less. Each bulletin provides an overview of a key supervisory topic; explains how supervisory staff members typically address that topic; highlights related policies and guidance, if applicable; and discusses examination expectations as appropriate at community banks. *FedLinks* is not intended to establish new supervisory expectations beyond what is already set forth in existing policies or guidance, but rather to connect policy with practice.

The most recently released *FedLinks* bulletin is:

"Interest Rate Risk Management," July 2015. This bulletin describes key risk management elements that are fundamental in a community bank's interest rate risk management program, describes examiner expectations when evaluating an interest rate risk management program, and includes a discussion of common interest rate risk management deficiencies.

This bulletin, and others like it, can be found online at www.cbcfrs.org/fedlinks.

By subscribing to *FedLinks* bulletins at www.cbcfrs.org/subscribe, you will receive an e-mail notification when new bulletins become available.

What Explains Low Net Interest Income at Community Banks? *continued from page 7*

The base model also includes variables that capture "interactive" effects between the interest rate and balance sheet variables.[5] The effect of changes in interest rates on net interest income may depend on the size of balance sheet items. For example, if the loan-to-asset ratio is relatively high, an increase in interest rates may cause interest income to rise more than if the loan-to-asset ratio is low, because loan rates are typically higher than the returns on other assets. The base model assumes the relationship between each variable and net interest income does not change over the entire sample period; that is, the recent recession and expansion are not fundamentally different from any other recession and expansion in the sample period.

Results from the base model are summarized in the first (1) column of Table 3. The top half of the table shows the estimated immediate effects of a 100-basis-point increase in each variable on net interest income, holding constant all other factor values. Because a change in the variables generally takes time to fully affect net interest income, the table also shows the cumulative effects, which are shown in the bottom half of the table. Approximately 80 percent of the cumulative effects occur within two years of a change in the value of a factor, and about 90 percent within three and a half years.[6]

The main findings of the base model indicate that community

[5] The interactive effects in the base model are the interest rates multiplied by the levels of balance sheet items. The base model also includes two lags of net interest income, to account for the persistence in net interest income, and other variables to control for other factors that affect net interest income. For the complete base model specification and estimated results, see Morris and Regehr (2014).

[6] Table 3 focuses on the primary variables of interest for this article. See Morris and Regehr (2014) for all the results. As noted in the text, the base model allows for the effect of interest rates on net interest income to depend on the levels of balance sheet items and vice versa. In Table 3, the immediate and cumulative effects of interest rates and balance sheet items include both the direct and interactive effects.

Table 3: Net Interest Income Regression: Immediate and Cumulative Effects

Select Variables	Base Model 1977:H1–2014:H2 (1)	Financial Crisis Break Model: Precrisis 1977:H1–2007:H1 (2)	Financial Crisis Break Model: Postcrisis 2007:H2–2014:H2 (3)
Immediate Effects in Basis Points (due to a 100-basis-point increase in factor)			
↑ 1-Year U.S. Treasury Rate	1.4	0.7	2.7
↑ 10-Year U.S. Treasury Rate	3.6	3.9	1.0
↑ (Parallel) in Yield Curve	5.0	4.6	3.7
↑ Loan-to-Asset Ratio	1.1	1.1	1.2
↑ Nonmaturity Deposit-to-Total Liability Ratio	1.1	1.2	0.4
Cumulative Effects in Basis Points			
↑ 1-Year U.S. Treasury Rate	4.1	2.0	8.0
↑ 10-Year U.S. Treasury Rate	10.4	10.8	2.9
↑ (Parallel) in Yield Curve	14.5	12.8	10.9
↑ Loan-to-Asset Ratio	3.0	2.9	3.4
↑ Nonmaturity Deposit-to-Total Liability Ratio	3.1	3.4	1.0

Note: For all model results, see Morris and Regehr (2014).

banks are asset sensitive on average. A parallel increase in the yield curve and an increase in long- and short-term rates are estimated to increase net interest income, which is consistent with the asset-sensitivity effects in Table 2. For example, the estimated immediate effect of a 100-basis-point parallel increase in the yield curve is a 5-basis-point increase in net interest income. As expected, an increase in the loan-to-asset or nonmaturity deposit-to-liability ratios increases net interest income, which supports the importance of lending and the deposit mix for community bank net interest income.

The cumulative effects provide a good measure of the degree to which the effects of the variables on net interest income are economically meaningful. In general, we found the sizes of the cumulative effects to be economically meaningful.[7] For example, the estimated cumulative effect of a 100-basis-point percentage-point parallel increase in the yield curve is a 14.5-basis-point increase in net interest income, with about 12 basis points of the increase occurring within 2 years. Thus, the base model results combined with low interest rates, fewer lending opportunities, and a relatively flat yield curve during all or some of the years since the start of the financial crisis and recession are consistent with the persistently low net interest income at community banks.

Has the Behavior of Net Interest Income Changed Since the Crisis?

To allow for the possibility that the decline in net interest income is out of the ordinary, a second model is estimated — the financial crisis break (FCB) model. The FCB model includes the same variables as the base model but allows for the possibility that their estimated effects on net interest income change after the start of the financial crisis in the second half of 2007.

The FCB model's results are shown in the second (2) and third (3) columns of Table 3. The estimated effects are consistent with the banks being asset sensitive in both the pre- and postcrisis periods, and the balance sheet items have the expected positive signs in both periods.[8] The sizes of the cumulative effects generally are economically meaningful in both periods.

[7] Formal statistical tests show that the estimated immediate effects of the variables are different from zero with a high degree of confidence.

[8] Formal statistical tests show that the estimated immediate effects of the variables are different from zero with a high degree of confidence. For the complete FCB model specification and estimated results, see Morris and Regehr (2014).

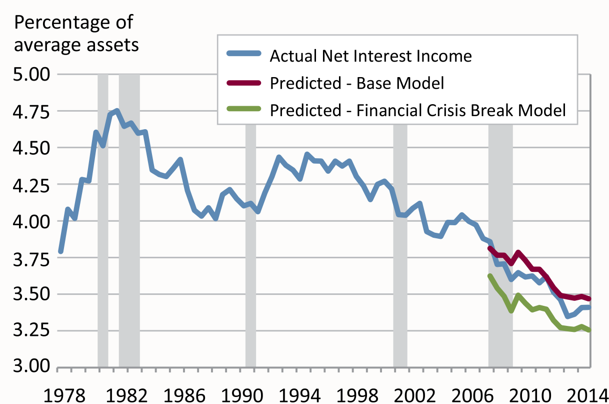
The estimated immediate and cumulative effects appear to have changed somewhat in the postcrisis period.[9] Some of the effects are smaller in the postcrisis period and others are larger. The largest changes in the cumulative effects are the 1-year Treasury rate (+6 basis points) and the 10-year Treasury rate (–7.9 basis points). Thus, based on these results, it is unclear whether the FCB model is better than the base model in explaining why community bank net interest income remains so low.

One way to determine if the relationship between community bank net interest income and the variables has changed is to see whether the base or FCB model is a better predictor of net interest income in the postcrisis period (Figure 2).[10] The FCB model (green line) underpredicts community bank net interest income over the postcrisis period with a relatively constant gap and, overall, predicts a 62-basis-point decline from the first half of 2007 relative to an actual decline of 47 basis points. In other words, even though community bank net interest income is already near a 40-year low, the FCB model predicts it should be 15 basis points lower. Although

[9] It is not possible to determine if the changes are statistically significant for technical reasons related to the interactive effects in the model.

[10] The predictions are out-of-sample predictions of community bank net interest income from the second half of 2007 to the second half of 2014. The out-of-sample predictions use the actual values of the variables but the predicted values of lagged net interest income.

Figure 2: Community Bank Net Interest Income: Actual and Predicted Values



Source: Consolidated Reports of Condition and Income
Notes: Sample net interest income (semiannual) annualized as a percentage of average assets over the previous year. The shaded bars depict recession quarters. See Morris and Regehr (2014) for a description of the data and estimation details.

the base model (dark red line) generally overpredicts net interest income, the predictions are more reasonable. The predicted value of net interest income in the second half of 2014 is just 6 basis points greater than the actual value, so the overall decline in net interest income over the prediction period is much closer to the actual decline than in the FCB model. A summary measure of predictive errors is the "root-mean-square error" (RMSE).[11] The RMSE of the base model is 8 basis points, which is more than 50 percent better than the 18 basis points of the FCB model. Thus, the base model appears to forecast somewhat better than the FCB model, suggesting the behavior of net interest income in the current recovery may not be that unusual given historical experience.

Table 4: Hypothetical Predicted Net Interest Income

Select Variables	2014H2 (percent)	Average 2004–2006 (percent)
Real GDP Growth Rate	2.50	3.22
Inflation Rate	1.29	2.62
1-Year U.S. Treasury Rate	0.13	3.48
10-Year U.S. Treasury Rate	2.39	4.45
10-Year–1-Year U.S. Treasury Rate	2.26	0.97
Loan-to-Asset Ratio	59.8	64.1
Nonmaturity Deposit-to-Total Liability Ratio	63.8	50.9
Base Model Predicted Net Interest Income as of 2017H1[a]	--	3.79

Source: Consolidated Reports of Condition and Income
[a] The prediction assumes that the initial conditions for the variables are as of 2014H2 and that the variables change to the 2004–06 averages in 2015H1 and remain at that level.

How Would Net Interest Income Change If Key Variables Return to More Normal Levels?

To get a sense of how a return to more normal levels of the key variables might affect net interest income, the base model is used to estimate what net interest income would be if these variables returned to their 2004–06 average levels in the first half of 2015 and remained at those levels over the following two years (Table 4). The two-year time frame is chosen because approximately 80 percent of the cumulative effect of changes in the variables on net interest income would be realized by the first half of 2017. The base model predicts that net interest income would be 3.79 percent in the first half of 2017 — a 38-basis-point improvement from the current 3.41 percent — although it would still be 19 basis points below the 2004–06 average.

Summary

This analysis shows that the lack of recovery in community bank net interest income in the seven years since the start of the financial crisis and recession is not unusual given economic and banking conditions. The regression results from the base model indicate that low interest rates, fewer lending opportunities, and a relatively flat yield curve during all or some of the years since the start of the financial crisis and recession have contributed to the current low levels of net interest income. These results also suggest, however, that low net interest income is not the new normal for community banks. Although net interest income may be unlikely to return to the high levels of the early 1990s, as the economy improves, net interest income is likely to rebound significantly. ■

[11] The root-mean-square error is defined as the square root of the sum of the squared prediction errors.

The Federal Reserve Board issued a final rule amending Regulation D (Reserve Requirements of Depository Institutions). This rule makes changes to the calculation of interest payments on excess balances maintained by depository institutions at Federal Reserve Banks. A press release was issued on June 18, 2015, and is available at www.federalreserve.gov/newsevents/press/bcreg/20150618a.htm.

The federal bank regulatory agencies announced additional EGRPRA outreach meetings. The Federal Reserve and other bank regulatory agencies are engaging in a series of outreach meetings with bankers, consumer groups, and other interested parties to provide them with the opportunity to present their views on the regulations under review. A press release was issued on April 6, 2015, and is available at www.federalreserve.gov/newsevents/press/bcreg/20150406a.htm. An additional press release announcing an outreach meeting on August 4, 2015, at the Federal Reserve Bank of Kansas City focusing on rural banking issues was issued on July 6, 2015, and is available at www.federalreserve.gov/newsevents/press/bcreg/20150706a.htm.

The federal bank regulatory agencies seek further comment on the interagency effort to reduce regulatory burden. The federal bank regulatory agencies approved a notice requesting comment on a third set of regulatory categories — consumer protection; directors, officers, and employees; and money laundering — as part of their review to identify outdated or unnecessary regulations applied to insured depository institutions. The Economic Growth and Regulatory Paperwork Reduction Act of 1996 (EGRPRA) requires the federal bank regulatory agencies, as well as the Federal Financial Institutions Examination Council, to conduct a review at least every 10 years to identify outdated or otherwise unnecessary regulations. A press release was issued on May 29, 2015, and is available at www.federalreserve.gov/newsevents/press/other/20150529b.htm.

Governor Jerome H. Powell spoke at the Annual Community Bankers Conference sponsored by the Federal Reserve Bank of New York on May 14, 2015. His speech, "Regulation and Supervision of Community Banks," is available at www.federalreserve.gov/newsevents/speech/powell20150514a.htm.

Governor Daniel K. Tarullo gave opening remarks at the EGRPRA outreach meeting in Boston on May 4, 2015. His remarks are available at www.federalreserve.gov/newsevents/speech/tarullo20150504.htm.

Governor Daniel K. Tarullo spoke at the Independent Community Bankers of America 2015 Washington Policy Summit on April 30, 2015. His speech, "Tailoring Community Bank Regulation and Supervision," is available at www.federalreserve.gov/newsevents/speech/tarullo20150430a.htm.

The Federal Reserve Board and five other federal financial regulatory agencies issued a final rule that implements minimum requirements for state registration and supervision of appraisal management companies (AMCs). An AMC is an entity that provides appraisal management services to lenders or underwriters or other principals in the secondary mortgage markets. These appraisal management services include contracting with licensed and certified appraisers to perform appraisal assignments. A press release was issued on April 30, 2015, and is available at www.federalreserve.gov/newsevents/press/bcreg/20150430a.htm.

Maryann F. Hunter, deputy director of the Federal Reserve Board's Division of Banking Supervision and Regulation, testified before the U.S. House of Representatives Subcommittee on Financial Institutions and Consumer Credit at a hearing titled "Examining Regulatory Burdens — Regulator Perspective" on April 23, 2015. Her testimony is available at www.federalreserve.gov/newsevents/testimony/hunter20150423a.htm.

The Federal Reserve Board issued a final rule to expand the applicability of its Small Bank Holding Company Policy Statement and apply it to certain savings and loan holding companies. The policy statement facilitates the transfer of ownership of small community banks and savings associations by allowing their holding companies to operate with higher levels of debt than normally permitted. The final rule raises the asset threshold of the policy statement from $500 million to $1 billion in total consolidated assets. A press release was issued on April 9, 2015, and is available at www.federalreserve.gov/newsevents/press/bcreg/20150409a.htm.

Community Banking in the 21st Century | Research and Policy Conference

On September 30–October 1, 2015, the Federal Reserve System and the Conference of State Bank Supervisors (CSBS) will host the third annual Community Banking in the 21st Century conference at the Federal Reserve Bank of St. Louis.

More than 150 guests, including economists, lawyers, regulators, commissioners, and bankers, will gather to discuss the latest in academic research on community banking issues as well as the practical challenges facing community banks. Fed Chair Janet Yellen will open the conference on the afternoon of September 30. The entire conference will be available for viewing live via web stream at www.communitybanking.org.

The research papers to be presented at this year's conference will cover multiple academic disciplines, including economics, finance, and law. Each research session discussion will be moderated by an academic and will include a community banker discussant.

This year's conference will also include the release of the findings from a new national survey of more than 800 community banks in 38 states. Administered by state bank commissioners, the survey will focus on changes in mortgage lending, changes in product mix, compliance costs, technology costs, and expected merger and acquisition activity. The findings will be released on the second day of the conference. In addition, the University of Utah, the winning team of the CSBS's pilot Community Bank Case Study collegiate competition, will present its research.

Visit the conference web page at www.communitybanking.org to view a preliminary agenda, conference news, current research and analysis, and links to past conference materials.

Connecting with You

What banking topics concern you most? What aspects of the supervisory process or the rules and guidance that apply to community banks would you like to see clarified? What topics would you like to see covered in upcoming issues of *Community Banking Connections*?

With each issue of *Community Banking Connections*, we aim to highlight the supervisory and regulatory matters that affect you and your banking institution the most, providing examples from the field, explanations of supervisory policies and guidance, and more. We encourage you to contact us with any ideas for articles so that we can continue to provide you with topical and valuable information.

Please direct any comments and suggestions to www.cbcfrs.org/feedback.

TO KEEP YOU INFORMED

The Board Implements the Interlocks Act Through Regulations L and LL

The Interlocks Act (12 U.S.C. 3201 et seq.) prohibits individuals, defined as "management officials," from serving simultaneously at two or more unaffiliated bank holding companies (BHCs), savings and loan holding companies (SLHCs), banks, thrifts, trusts, credit unions (each a "depository organization"), or their affiliates if the depository organizations in question have offices in the same community, the same relevant metropolitan statistical area, or have total assets exceeding, on the one hand, $2.5 billion and, on the other hand, $1.5 billion. The Board implements the Interlocks Act through Regulation L (12 CFR 212) for BHCs, state member banks, and their affiliates, and through Regulation LL (12 CFR 238 subpart J) for SLHCs and their affiliates.

When considering a request for an exemption, the Board is required by statute and regulation to consider whether the interlock would substantially lessen competition, result in a monopoly, or present safety and soundness concerns. Recently, the Board stated that it "applies a strong presumption against granting a general exemption, and a general exemption request will only be granted in limited situations where warranted by the particular facts of the request"; see www.federalreserve.gov/bankinforeg/LegalInterpretations/bhc_changeincontrol20150218a1.pdf.

If you have any questions, call Alison Thro of the Board of Governors at 202-452-3236, or the Regulatory Applications officer at your Reserve Bank.

Compliance Requirements for Commercial Products and Services

The term "federal consumer protection laws" suggests that the scope of these laws is limited solely to consumer products and services. However, some of these laws — including the Equal Credit Opportunity Act (ECOA), the Flood Disaster Protection Act (FDPA), and the Servicemembers Civil Relief Act (SCRA), among others — also apply to commercial products and services. In addition, other federal consumer protection laws, although generally limited in scope to consumer products and services, include certain provisions that also apply to commercial products and services. For example, Regulation Z (the implementing regulation for the Truth in Lending Act (TILA)) includes certain requirements for business-purpose credit cards.

Employees at community banks with responsibility for commercial products and services should be aware of the requirements for their products and services. The First Quarter 2015 issue of *Consumer Compliance Outlook*, a sister Federal Reserve System quarterly newsletter that focuses on financial institutions' compliance with federal consumer protection laws and regulations, recently featured an article that discussed the compliance requirements for commercial products and services. Bankers are encouraged to read the article, which is available at consumercomplianceoutlook.org/2015/first-quarter/consumer-compliance-requirements-for-commercial-products-and-services/. The entire issue that contains the article is also available in PDF at consumercomplianceoutlook.org/assets/75b3d4fa92bf41c5b9d311e8f9d67430.ashx.

Interested in Reprinting a *Community Banking Connections* Article?

FEDERAL RESERVE SYSTEM

COMMUNITY BANKING

CONNECTIONS

Second Quarter 2015

VIEW FROM WASHINGTON

Some Thoughts on Community Banking:
A Conversation with Chair Janet Yellen

Advantages and Challenges Facing Community Banks

INSIDE

Please contact us at editor@communitybankingconnections.org. We generally grant reprint permission free of charge provided you agree to certain conditions, including using our disclaimer, crediting *Community Banking Connections* and the author, and not altering the original text.

Scan with your smartphone or tablet to access *Community Banking Connections* online.