DALLASFED

VOLUME 3, ISSUE 4
DECEMBER 15, 2014

Financial Insights

FIRM • FINANCIAL INSTITUTION RELATIONSHIP MANAGEMENT

DALLAS FED RESOURCES

Economic Updates

Regional—"Regional Outlook Remains Upbeat"

National—"U.S. Growth Pace Moderate; Inflation Low, Employment Data Mixed"

International—"Global Outlook Weakens"

Publications

Community Banking Connections

Dallas Beige Book
December 2014 Summary

Economic Letter
"Are We There Yet? Assessing Progress Toward Full Employment and Price Stability"

Southwest Economy
"Budget Balancing Act: Health and Education Stretch Texas Resources"

Surveys & Indicators

Agricultural Survey

Texas Business Outlook Surveys—Manufacturing, Service Sector, Retail

Texas Economic Indicators

Webcasts

Economic Insights: Conversations with the Dallas Fed
"The Federal Reserve and Financial Services: Past, Present, Future"

Find other resources on the Dallas Fed website at www.dallasfed.org.

Payments: A Changing Landscape

by Matt Davies

The Federal Reserve Banks have a long-standing mission of fostering the integrity, efficiency and accessibility of the U.S. payments system. The payments landscape is changing rapidly, and it is more critical now than ever that a financial institution's management team, board of directors, employees and customers (businesses and consumers) are up to speed on the latest trends in payments. This article highlights some of the most important issues in payments today.

Cybersecurity: Protecting Payments

Ask a community bank or credit union CEO what keeps him or her awake at night, and among the likely responses is "cybersecurity." Data from PriceWaterhouseCoopers indicate that the number of reported information security incidents around the world in 2014 rose 48 percent to 42.8 million, the equivalent of 117,339 attacks per day. The victims of many of the highly publicized incidents in the U.S. in 2014 were retailers, but surely banks and credit unions felt more than the usual level of discomfort when, in July of this year, JPMorgan Chase announced that it had suffered a breach.

It is at the intersection of cybersecurity and payments where incidents can become particularly devastating, in what is referred to as corporate account takeover. Business customers are using PCs to connect with financial institutions to initiate online banking sessions, through which they will send wire transfers or originate ACH transactions. Unfortunately, at most businesses, those PCs are not dedicated solely to online banking; employees are using them to surf the web, check personal email and visit social media sites. They may open email attachments that will execute malicious software ("malware") or click on links to websites that are in the control of hackers, who then plant key-logging software on the PC and capture the credential of the user the next time he or she logs in to online banking. The hackers can then "take over" the account to initiate fraudulent wires or ACH transactions.

To help reduce opportunities for hackers to take over corporate accounts, banks and credit unions must maintain an awareness of the latest developments in online banking malware. In addition, the importance of using multifactor authentication for online banking was stressed in the Federal Financial Institution Examination Council's (FFIEC)[1] 2011 supplemental guidance to Authentication in an Internet Banking Environment. Unfortunately, no matter how vigilant the financial institution is, it may be that a customer or member is the weakest link. Financial institutions should educate their business customers on trends in payments fraud and cybersecurity as well as methods for protecting themselves and preventing corporate account takeover.

In this summer's verdict in *Choice Escrow & Land Title LLC v. BancorpSouth Bank*, the Eighth Circuit Court of Appeals not only ruled in favor of a bank that had been sued by its corporate customer in a corporate account takeover case, but also allowed the bank to attempt to recoup its legal fees from the corporate customer. The case arose from an account takeover incident exacerbated by the corporate customer not having dual control requirements in place for wire transfers; the corporate customer had even declined the use of dual control in writing. In light of this case, many financial institutions are reviewing their agreements with customers for the provision of cash management services and ensuring the agreements are in order.

CALENDAR OF EVENTS

Feb. 17
Economic Roundtable
Paris, Texas

Feb. 20
Economic Roundtable
Dallas, Texas

Feb. 27
Economic Roundtable
Plano, Texas

March 4
Economic Roundtable
Fort Worth, Texas

March 5
University Presentation
Stephenville, Texas

March 17
Economic Roundtable
Midland, Texas

March 25
Community Depository Institutions Advisory Council Meeting
Dallas, Texas

For more information about these events, email FIRM at Dallas_Fed_Firm@dal.frb.org.

In other cybersecurity news this year, the National Institute of Standards and Technology (NIST) released its Framework for Improving Critical Infrastructure Cybersecurity in February. Though the document is a useful resource, compliance is voluntary, and many financial institutions have not paid it much attention. A Treasury Department official recently indicated that a version 2.0 would be released at some point and that there may be associated with its release some type of incentives for financial institutions to comply, which could take the form of "discounted cybersecurity insurance and some degree of regulatory streamlining."[2]

More recently, in November, the FFIEC released its Cybersecurity Assessment General Observations, based on a cybersecurity assessment piloted at over 500 community financial institutions to evaluate their preparedness to mitigate cyber risks. The document provides an overview of the risks and risk management practices among financial institutions. The questions the document poses can be used by CEOs and boards of directors for assessing their own institutions' cybersecurity preparedness.

Apple Pay and Mobile Wallets

On Oct. 20, Apple launched its mobile payments service, Apple Pay, which can be used on the latest iPhone models, the 6 and 6 Plus. For some time, the conventional wisdom with mobile payments had been that, to motivate consumers to use mobile payments, providers needed to use discounts, offers and/or loyalty functions. Apple turned that model on its head, as there is no offers/loyalty component with Apply Pay (at least not yet). Instead, Apple Pay is all about security. And the timing probably could not have been better. In the last year, consumer cardholders have become increasingly aware of data breaches and the reissuance of cards that often follows. Consumers are looking for more control of their personal and financial information, and Apple Pay offers consumers several attractive security features. First, by using tokenization, the actual credit card number is never stored on the iPhone; instead, the number stored is a tokenized, "device-only" account number. The merchant never sees the real card number. The data stored by the merchant is thus "devalued"—it is of no use to hackers as it cannot be used to create new physical cards. In addition, Apple Pay uses multifactor authentication for transactions, combining something the consumer has (the iPhone) and something the customer "is" (a thumb- or fingerprint through Apple's TouchID).

On Visa's website is a list of financial institutions—many of them community banks and credit unions—that plan to offer Apple Pay. As of Nov. 3, the list included 317 credit unions and 120 banks. Financial institutions might want to check out that list to see if the competitor community bank or credit union down the street is on it. It remains to be seen whether Apple Pay will be successful and, if it is, if "a rising tide will lift all boats," that is, whether the entry of Apple into mobile payments heralds growth for others in the market—like Google Wallet, Softcard (formerly Isis Mobile Wallet, a joint venture of AT&T, T-Mobile and Verizon) and Merchant Customer Exchange's (MCX) mobile wallet, CurrentC. Regardless of the vendor or provider, financial institutions may want to have a plan for facilitating the ability of their customers to make payments through their mobile phones.

EMV

We are now less than a year away from the Oct. 1, 2015, "liability shift" associated with the implementation of the Europay–MasterCard–Visa (EMV) standard in the U.S. After that date, the party that is not able to facilitate a chip-card transaction—either the issuing bank or merchant—can be held financially liable for fraud losses from card-present counterfeit fraud at the point of sale. In an EMV-enabled transaction, the chip in the card generates "dynamic data" unique to the transaction so the data stored by the merchant, if compromised, cannot be used by hackers to create new physical cards.

The liability shift was intended to foster adoption of EMV-enabled terminals at merchants and issuance of chip cards by banks and credit unions. However, recent research from Javelin Strategy & Research indicates that only about 1.5 percent of the approximately 1.2 billion payment cards in the U.S. have a chip, and only 10 percent of merchant terminals are EMV-enabled.[3] While some large banks have begun to issue EMV-enabled cards, many community banks and credit unions will not be able to do so until late 2015, or even later, depending on the

schedules of vendors/processors. Perhaps it will be some consolation that many merchants, especially small and midsize ones, also will not have upgraded their terminals by October 2015.

As stated earlier, it is important for financial institutions to educate their customers, and the EMV implementation provides a great opportunity to do so. The U.S. EMV implementation is being referred to not as "chip-and-PIN," but as "chip-and-choice," meaning that a financial institution (or its processor) will make the decision as to whether the EMV cards it issues (or its processor issues on its behalf) will require the use of a PIN or will allow for signature as a cardholder verification method. Financial institutions will need to let their customers know which option they have chosen (and perhaps why) and that this may be different from cards received from other banks or credit unions. (Note that JPMorgan Chase and the federal government have both announced plans to go the "chip-and-PIN" route.)

When a consumer uses a chip card at a point-of-sale terminal that is EMV-enabled (Walmart, for example, has turned on EMV acceptance at all of its U.S. stores), if the consumer tries to swipe the card, the terminal will indicate that it cannot read the card and that the card must be inserted into the terminal. This is referred to as "dipping" the card. The card must remain in the terminal for the duration of the transaction, until the terminal indicates that the card can be removed. In countries where EMV has been more fully implemented, such as Canada, this has led to consumers leaving cards in terminals when they leave a store.

Financial institutions should take the opportunity to talk with their customers or members about their plans for EMV. Consumers generally have become more aware of the need for enhanced security for credit cards, so they will value communication from their financial institutions about EMV and how it will help to protect their cards.

Mobile Banking

Mobile remote deposit capture (mRDC) offers another opportunity for communicating with and educating customers. Many community banks and credit unions have indicated that offering mRDC is an essential part of their mobile banking offerings. A November 2014 report issued by the Pew Charitable Trusts, Terms and Conditions of Mobile Remote Deposit Capture: The Disclosure Practices of Banks and Prepaid Card Companies, identifies 10 areas in which the terms of mRDC products are poorly disclosed or basic features, such as notifications regarding the status of deposited funds, are not available. The report suggests that, if a financial institution communicates more clearly with its customers or members about funds availability on transactions, for example, it can enhance their confidence in mobile banking.

Ongoing awareness of developments in payments offerings—in mobile banking and elsewhere—is extremely important. With mobile banking, a number of financial institutions are taking imaging technology beyond mRDC to mobile photo bill pay. They are also offering customers or members the ability to use mobile banking to turn a debit card off and on. In some cases, consumers are using this feature to keep their debit cards off until right before making a purchase and then turn them back off after doing so. Herein lies yet another chance for a financial institution to educate its customers or members and to be viewed as offering the most up-to-date technology for protecting customers during transactions.

Matt Davies, AAP, CTP, CPP, is payments outreach officer in the Financial Institution Relationship Management Department at the Federal Reserve Bank of Dallas. Send comments or questions about this article to him at matt.davies@dal.frb.org.

NOTES

The views expressed herein are those of the author and not necessarily those of the Federal Reserve Bank of Dallas or the Federal Reserve System. They do not constitute legal advice.

[1] Members of the FFIEC are the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corp., the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau, the National Credit Union Administration and the State Liaison Committee.

[2] "Feds May Dangle Carrot for Banks to Adopt Cybersecurity Framework," by John Reosti, *American Banker*, Nov. 17, 2014.

[3] "Warning: The EMV Chip Card Conversion Will Be Slow and Fraught with Peril," by Jim Daly, *Digital Transactions News*, Oct. 7, 2014.

ABOUT *FINANCIAL INSIGHTS* AND FIRM

Financial Insights is published periodically by FIRM – Financial Institution Relationship Management – to share timely economic topics of interest to financial institutions.

FIRM was organized in 2007 by the Federal Reserve Bank of Dallas as an outreach function to maintain mutually beneficial relationships with all financial institutions throughout the Eleventh Federal Reserve District. FIRM's primary purpose is to improve information sharing with district financial institutions so that the Dallas Fed is better able to accomplish its mission. FIRM also maintains the Dallas Fed's institutional knowledge of payments, engaging with the industry to understand market dynamics and advances in payment processing.

FIRM outreach includes hosting economic roundtable briefings, moderating CEO forums hosted by Dallas Fed senior management, leading the Dallas Fed's Community Depository Institutions Advisory Council (CDIAC) and Corporate Payments Council (CPC), as well as creating relevant webcast presentations and this publication. In addition, the group supports its constituents by remaining active with financial trade associations and through individual meetings with financial institutions.

MEMBERS OF FIRM

Tom Siems
Assistant Vice President and Senior Economist
Tom.Siems@dal.frb.org

Jay Sudderth
Assistant Vice President
Jay.Sudderth@dal.frb.org

Matt Davies
Payments Outreach Officer
Matt.Davies@dal.frb.org

Steven Boryk
Relationship Management Director
Steven.Boryk@dal.frb.org

Ericka Davis
Senior Economic Outreach Specialist
Ericka.Davis@dal.frb.org

Donna Raedeke
Payments Outreach Analyst
Donna.Raedeke@dal.frb.org

Contact us at Dallas_Fed_FIRM@dal.frb.org.

Noteworthy Items

President Richard Fisher announces plans to retire
Dallas Fed President and CEO Richard Fisher announced that he will retire from his position on March 19, 2015. The board of directors of the Federal Reserve Bank of Dallas has retained the executive search firm of Heidrick & Struggles to conduct a search for a new president. READ MORE

Federal Reserve System releases the 2014 Payments Fraud Survey report
During 2014, FIRM conducted a survey on payment-related fraud experienced by financial institutions and corporations within the Eleventh District. This report was part of a broader initiative conducted in conjunction with several other Federal Reserve Districts. READ MORE

President Fisher provides remarks before the Shadow Open Market Committee, Manhattan Institute, New York City (Nov. 3, 2014)
"The happy outcome to our economic predicament would entail the marriage of sensible fiscal policy with prudent monetary policy, carrying the American economy to new horizons, allowing the Fed to emerge a hero. One can envision less-pleasant outcomes, however, some of them tragic." READ MORE