2019

Innovation in Electronic Fund Transfers and Associated Consumer Compliance Risks

A CASE STUDY ON ZELLE

LISAMARIE NG-KREITER, FIELD EXAMINATION MANAGER, CONSUMER FINANCIAL PROTECTION BUREAU

Table of Contents

Executive Summary

The Consumer Financial Protection Bureau (CFPB) is responsible for the supervision and enforcement of the Electronic Fund Transfer Act (EFTA), as implemented by Regulation E. The EFTA establishes the basic rights, liability, and responsibilities of consumers who use electronic fund transfer services, and of financial institutions that offer these services. The EFTA includes requirements for institutions and service providers for peer-to-peer payments. As payment systems progress, and provide consumers with faster and different ways to send money, CFPB examiners should adapt to understand how to assess the changes, and applicable regulatory requirements.

In October 2016, Early Warning, a bank-owned partnership, announced the launch of Zelle. Zelle is a digital payments network that allows consumers to send money directly from their bank accounts or debit cards to another consumer. Zelle has changed the speed at which consumers can send money, and shifted information sharing across financial institutions. As such, examiners need to be nimble in their ability to comprehend the Zelle structure and in determining the applicability of EFTA in order to regulate the product.

The CFPB examination procedures for assessing compliance with Regulation E fail to capture all of the requirements pertaining to Early Warning and the financial institutions that engage Zelle. The examination procedures currently include general questions for examiners to determine if a transaction is an EFT as defined by Regulation E, and whether the financial institution processed the transaction in accordance with regulatory requirements. The procedures do not reference the liability requirements for third parties, like Early Warning, and are not clear

on expectations for ensuring that the Zelle network contains accurate information for sending payments to the correct recipient.

In order to keep pace with advancements in payments systems, the examination procedures should include guiding questions for assessing EFTs, and additional support for understanding the party responsible for complying with the regulatory requirements. The tools at examiner disposal, including exam procedures, bulletins, and findings on public enforcement actions serve to direct examiners to possible areas of risk, and how prior actions may dictate future responses. Those tools, although useful in setting expectations, do not provide sufficient guidance. In order to ensure that examiners have appropriate tools, the Bureau should update examination procedures and training. By updating the examination procedures to include all of the EFTA requirements, examiners will have access to materials that can be applied to Zelle, and other advancements in the P2P market. Procedures help to drive consistency across examinations at multiple institutions, and across similar products. They clarify and assist examiners in scoping and administering reviews. Other regulators that examine Zelle at institutions not within the CFPB's jurisdiction can also leverage them. Procedure updates will serve as a signal to the financial marketplace that regulators are nimble, and ready to review and understand how these products work, and the impact on the consumer.

Part I: Statement of Problem/Hypothesis

A payment system is a structure that governs the clearing, settlement, and recording of payments within the financial marketplace, and includes agreements between three or more parties.[1] Payment systems include written rules and procedures for all participants. As payment systems continue to evolve, it is important to understand the impact on the consumer and the application of the law. The Consumer Financial Protection Bureau (Bureau or CFPB) supervises institutions for compliance with the Electronic Fund Transfer Act and determines whether unfair, deceptive, or abusive acts or practices are occurring by the parties in the payment systems. The Bureau has supervisory authority over depository institutions with over $10 billion in assets, and larger participants in the non-depository area. Payment systems include relationships across depository institutions, non-depository institutions, and service providers. In order to ensure that consumers are treated fairly, the Bureau should also understand these relationships, the applicability of regulations, and the areas for potential consumer harm.

An electronically created payment involves a merchant payment instruction placed into an electronic file, which then processes through the check-clearing network. Electronic payments do not begin with paper, as they are initiated through Internet or telephone instructions from the consumer. Electronic peer-to-peer (P2P) payments are a type of electronic payment and have existed for almost 20 years. They were first created by online auction websites to enable faster payments. Before its creation, payments were usually completed with a paper check through the mail. This included a risk of nonpayment. Electronic P2P payments are usually associated with a

[1] Board of Governors of the Federal Reserve System, "The Federal Reserve Policy on Payment System Risk (PDF)" (Washington: Board of Governors, 2016).

consumer deposit account for recurring or one-time debit transactions. Electronic P2P payments typically use traditional payment networks for funds transfer. A common example is when a person makes a payment and the receiver has an account at the same bank. This is called an "on us" transaction, and it is settled by posting entries on one institution's books[2]

There are three types of P2P payment models. The first is a nonbank-centric model where the consumer tells the nonbank intermediary to transfer funds to another consumer. An example of this is PayPal. The second model is the bank-centric model, where the consumer tells the bank to transfer money from one bank account to another consumer's bank account. The third model is card-centric, where the payment processing occurs over a credit card or debit card network.[3] The research sources relied upon examine how these models transformed over time based on consumer need. The focus of this paper is on the bank-centric model.

History of P2P

In 1998, PayPal set up a P2P payments system by allowing consumers to use their checking account or a debit or credit card to make faster payments. PayPal paid each new customer $10, and a $10 referral fee to existing customers. PayPal estimated between $6 million and $8 million P2P payments occurred daily in 1999. The mobile P2P payments market is estimated to hit $174 billion per year by 2019.[4]

[2] FFIEC, "Retail Payment Systems Handbook," *Board of Governors of the Federal Reserve System*, 2016.
[3] Bradford, Terri and William Keeton, "New Person-to-Person Payment Methods: Have Checks Met Their Match?," *Federal Reserve Bank of Kansas City*, 2012.
[4] Bradford, Terri, "Banks Re-enter the P2P Payments Fray: With Mobile, Will this Time Be Different?" *Federal Reserve Bank of Kansas City,* 2012.

In 2000, Wells Fargo Bank collaborated with eBay to offer Billpoint. Billpoint was a free P2P payment method where eBay buyers could use a credit card and maintain account number privacy. A few months after its launch, eBay purchased Wells' share and charged fees per sale and as a percentage of the total sale. In the same year, other banks entered the payments market. Bank One developed eMoneyMail, which allowed consumers to pay using an email address. Citibank developed c2it with AOL. Both products used a checking account, or debit or credit card, and charged flat rates per transaction. Bank One canceled eMoneyMail within six months due to high rates of fraud, while Citibank made c2it free, to compete with PayPal. In 2002, 70 percent of eBay auctions accepted PayPal, while only 27 percent accepted Billpoint. eBay closed Billpoint, and purchased PayPal in 2002. Citi closed c2it in 2003. In March 2002, the New York Cash Exchange, an interbank network connecting ATMs in the United States and Canada, announced a real-time P2P payment through ATMs. Customers could use their ATM card number to pay from their home computers, ATMs, virtual response units, and personal digital assistants. The service never launched in the U.S. because of concerns around sharing ATM information. By 2015, PayPal had 192 million active users across platforms, including mobile, and 4.9 billion transactions, totaling $282 billion. Of those transactions, $66 billion were made on a mobile device. In the third quarter of 2018, PayPal reported $2.5 billion in total payment transactions.[5]

As the payments market grew, non-bank P2P providers entered the market. Products such as Venmo, Facebook Messenger, Square Cash, and Google Wallet began offering free platforms for sending money. Venmo is a PayPal subsidiary that targets millennials. Payments are made

[5] (PYMNTS, 2018) PYMTS, "PayPal Posts 25 Pct Jump In Payments Volume," *PYMTS*, 2018. https://www.pymnts.com/earnings/2018/paypal-stocks-payments-transaction-volume/ (August 20, 2018).

via a mobile app, or through Venmo's website. Users link their bank account or credit or debit card, and transfer money to their social contacts. Recipients are able to either maintain a balance, or transfer it to their bank account within one to two business days. In 2016, Venmo processed $12.1 billion in transactions. Facebook Messenger allows users to send money at no cost, and receive the payment in their accounts within three business days. Square Cash P2P allows users to transfer funds to a bank through the linking of a debit or credit card. Debit card transactions are free, and credit card transactions are charged three percent. Square Cash uses email, the Spare Cash app, internet links, or Bluetooth. Payments process within one or two business days. Google Wallet provides free transactions between bank accounts and the Wallet. Google charges a 2.9 percent transaction fee for payments made with debit or credit cards. Funds take up to three business days to reach the bank account. Dwolla partnered with mFoundry, a subsidiary of FIS, to enable mobile payment platforms and real-time transfers. Fiserv's Popmoney also enables P2P payments for more than 2,400 financial institutions.

In 2011, Bank of America, JP Morgan Chase, and Wells Fargo created clearXchange, a platform for P2P using the automated clearinghouse for settlement. The National Automated Clearing House Association (NACHA) governs the ACH network through the administration, development, and enforcement of operation rules. An ACH transaction includes an originator who initiates a direct deposit or direct payment transaction electronically. The originating depository financial institution enters the ACH entry for the originator, and aggregates payments from customers to transmit in batches at predetermined intervals. The ACH operator, the Federal Reserve or the Clearing House, receives the batches, sorts and make them available to the receiving depository institution. The receiving institution debits or credits the receiver within one

or two business days.[6] ACH fund transfers can be credit transfers in which funds are pushed or pulled between a payer's and payee's depository institutions. ACH credit and debit transfers have grown since 2012.[7]

Since its creation, other banks have joined ClearXchange. ClearXchange allows U.S. bank accountholders to send or receive money through mobile or online services for free using the recipient's email address or phone number. Recipients can access funds within five business days. Early Warning System, a real-time payment provider, acquired clearXchange in October 2015. In 2016, banks began using Early Warning's clearXchange, allowing for payment processing within minutes, and rebranded it under the name Zelle.

Zelle

Early Warning teamed with Fiserv, Inc., a financial services technology solutions provider, to launch ZelleSM Network in October 2016. The Zelle network offers a faster way to send and receive payments through the consumer's financial institution's security system. Fiserv offers all of the Zelle elements in a single platform, reducing costs and time. Fiserv and Early Warning reach over 6,000 banks and credit unions, including 40 of the largest financial institutions. Consumers access Zelle directly through their bank's mobile app and send or request money using an email address or phone number.[8] Zelle provides access to over 76 million mobile bank users nationwide. The Zelle Network includes Ally Bank, Bank of America, Bank

[6] (NACHA, 2018) NACHA, "ACH Network: How it Works," *NACHA The Electronic Payments Association,* 2018 https://www.nacha.org/ach-network (Accessed August 20, 2018).
[7] (Federal Reserve Bank of Atlanta, 2018) Federal Reserve Bank of Atlanta, "Federal Reserve Payments Study - 2017 Annual Supplement," *Board of Governors of the Federal Reserve System*, 2018.
[8] Business Wire, "Fiserv and Early Warning P2P Payments Alliance Gets Quick Start with Multiple Financial Institutions Committing to Early Warning's Zelle Network," *Business Wire*, 2016.

of the West, BB&T, BECU, Capital One, Citi, Fifth Third Bank, FirstBank, First Tech Federal Credit Union, Frost Bank, JP Morgan Chase, Morgan Stanley, PNC, USAA, U.S. Bank, and Wells Fargo. Early Warning partnered with CO-OP Financial Services, FIS, Fiserv, and Jack Henry for payment processing, and Mastercard and Visa for multiple pathways onto the network.[9] Zelle processed $199 billion in payments across 433 million transactions in 2018.[10]

As a payment system for both consumers and businesses, Zelle has the potential to negatively impact multiple parties. First, Zelle makes it difficult for consumers to change banks if their account is with a bank within the Zelle network. Users link their bank account to their phone or email address. If a consumer chooses to switch banks, their phone or email is still associated with the account number from the previous bank. Switching and re-engaging the relationship with a new bank can become cumbersome without proper controls. Second, it is unclear whether Zelle or the participating bank is responsible for resolving an error or fraud investigation. Consumers may complain to the wrong institution, and delay receiving refunds. Third, for consumers who use banks that do not participate in the Zelle network, liability and error resolution need to go through Zelle. As a regulator, it is important to understand Zelle because of the number of consumers it affects.

Zelle is shifting the payment systems market away from nonbank processors by providing real-time transfers across banks. Consumers whose banks do not participate in Zelle are still able

[9] Early Warning Services, "Early Warning Announces Zelle Network," *Early Warning*, 2016 HTTP://WWW.EARLYWARNING.COM/ABOUT-US.HTML (Accessed August 20, 2018).
[10] Early Warning Services, "Zelle® Ends 2018 with its Strongest Quarter on Record," *Early Warning,* 2019, https://www.zellepay.com/press-releases/zelle-ends-2018-its-strongest-quarter-record (Accessed January 30, 2019).

to use the service by enrolling their debit cards.[11] Zelle was projected to reach 27.4 million users by the end of 2018, compared to Venmo projected at 22.9 million users, and Square Cash projected at 9.5 million users.[12] Early Warning Services reported that Zelle processed 433 million transactions with $119 billion in payments in 2018. In 2017, Zelle had processed 247 million transactions with $75 billion in payments. For 2018, Zelle reported reaching over 100 million users through participating banks.[13]

As many of the key players within the Zelle network contain institutions over $10 billion in assets, it is imperative for the Bureau to understand how Zelle works, and its consumer impact. This paper will assess Zelle's strengths and weaknesses, and how the Bureau can extend supervisory authority to cover payment systems. The project will also review other regulator guidance on payment systems, and their reactions to Zelle. In 2015, the Bureau released its vision for consumer protection in new faster payment systems. The principles outline expectations for a safe, transparent, accessible, and efficient payment system keeping in mind consumer protection. In April 2017, the Bureau published amendments to Regulation E. The amendments pertained to prepaid accounts covered by Regulation E and Regulation Z. The major amendment added digital and mobile wallets that serve as a funding source for P2P payments to the definition of prepaid. Digital and mobile wallet providers must comply with disclosure requirements.

[11] American Bankers Association, "Understanding Zelle," *ABA*, 2018 https://www.aba.com/Tools/Function/Technology/Documents/UnderstandingZelle.pdf (Accessed August 20, 2018).
[12] Clark, Doug, "Zelle to OVertake Venmo in 2018," *eMarketer,* 2018 https://www.emarketer.com/newsroom/index.php/zelle-to-overtake-venmo-in-2018/ (Accessed August 20, 2018).
[13] Early Warning Services, 2019.

The research relied upon in this paper may be applied to current initiatives in understanding how to treat Zelle and other payment systems. It may also be used to update examination procedures and how examiners review both the banks participating in the Zelle network, and the Zelle service. It will identify areas to examine, and ways to drive consistency in our review of Zelle. It will also help inform other regulators on the service, as well as understand expectations for institutions that engage with Zelle.

The paper will determine whether the current examination procedures for assessing compliance with Regulation E fail to consider the nuances of Zelle, and fail to adequately cover the questions and possible concerns with the Zelle network. It may be used to understand and evaluate other similar payment systems, and support consistency in how these services are treated. As innovations in the financial marketplace and payment systems continue to provide faster and easier methods of interacting, federal consumer financial laws and regulations need to update and enhance their scope of focus in order to protect consumers.

Part II: Research Methodology: Data Sources and Analysis

Zelle, and other P2P payment services are a topic of continual study and analysis by banking associations and regulator publications. As regulators contemplate how to best examine advancing payments systems, there is a need to understand how new payment systems operate and how financial institutions are employing them. A number of journal and news articles, published reports, regulator procedures, and company user agreements were used to assess Zelle's operations and extrapolate regulations that may apply.

The research included a review of the Bureau's examination procedures and the FFIEC examination procedures. The FFIEC Retail Payment Systems examination procedures were

updated in 2016, and the Bureau's Electronic Fund Transfer Act procedures were updated in 2013. Neither directly contemplates the use of a service that incorporates bank cooperation in delivering P2P payments. In addition, the FFIEC Retail Payment Systems examination procedures state that emerging payment systems, like Zelle, need further analysis. The procedures contain a section that references and defines areas of concern, but do not provide the same in-depth analysis used with mature payment systems.

The American Bankers Association, the Electronic Funds Transfer Association, the Electronic Transactions Association, NACHA –The Electronic Payments Association, The Clearing House, and Card Network Services are examples of organizations that have contemplated the evolution of payments systems, and next steps. A review of these publications guidance, opinions, and statements on electronic P2P payments was also performed.

The research constraints include access to Zelle's management team, and management at banks that engage with Zelle. As a regulator, it was inappropriate to approach banks and Zelle management requesting information. The research was also limited to the public decisions made by regulators. Confidential examination work may be ongoing, and the results are not available to the public. As such, only publicly available information on updates to regulations and analysis was utilized.

The methods to gather and present research information include searches of online periodicals and public actions. Published reports from other regulators were heavily relied upon in this research paper. Those reports show the evolution of payment systems, and their strengths and weaknesses. They also contemplated how to regulate each system as it evolves. Past regulator analyses on older payment systems, such as check, ACH transfers, and nonbank centric

models provide a basis for understanding how these systems have been treated in the past and provide examples of how Zelle may be regulated.

The review also compared Zelle's bank consortium to the entity governing ACH transactions. NACHA, which governs the use of ACH transfers, has guidelines in how to interact in the system, and enforce requirements. A self-governing model for Zelle, similar to NACHA, could serve as a way to ensure the proper controls and measures are taken by banks in protecting consumers. System rules and identification of actors will help identify who is responsible for ensuring proper controls and understanding of risk.

Part III: Findings and Conclusions

The Bureau and the FFIEC published examination procedures for guiding examiners in their review of institution compliance with the Electronic Fund Transfer Act (EFTA), and effectiveness of an institution's compliance management system (CMS) as it relates to payment processing and electronic banking (E-banking). This paper assesses those procedures, their applicability when evaluating Zelle, and the treatment of Zelle's main competitor.

The examination procedures applicable to a review of Zelle's services are the EFTA procedures and the CMS procedures, both located in the Bureau's examination manual. The EFTA procedures were updated in October 2013, and the CMS procedures were updated in August 2017. Electronic P2P payments were introduced in 1998, and expanded in 2016 to include non-bank providers. Both the EFTA and the CMS procedures do not address advances within the electronic fund transfer space. In addition, the procedures do not provide guidance in determining who is ultimately responsible for compliance when another party processes the transfer.

EFTA and its implementing Regulation E established a framework of rights, liabilities, and responsibilities of participants in the electronic fund transfer systems. Regulation E's Subpart A includes requirements for disclosures, error resolution, and rules related to unauthorized electronic transfers. In October 2016, the Bureau issued amendments to Regulation E, establishing protections for consumers with prepaid accounts, and made clerical and non-substantive corrections. As Zelle is an electronic fund transfer service, certain requirements of Subpart A of Regulation E apply.

Zelle's Requirements Under Regulation E

Zelle can be used by both network participating and non-participating banks. Institutions within the Zelle network should be clear on who is responsible for compliance with Regulation E, and how they will ensure that consumers are protected. Zelle's requirements under Regulation E differ depending on where the consumer account is held. If the consumer's account is with a participating bank, liability and error resolution requirements rest with the consumer's bank. If the consumer links an account from a non-participating bank, Zelle becomes a service provider, and must follow the liability and error resolution requirements of Regulation E.

For network participating banks, Zelle is directly connected to a consumer's bank account. Since it is already a feature of mobile banking, the consumer does not need to expose account information to a third party. They are able to use the service through the security network of their bank. In addition, the recipients are able to obtain funds without having to enroll in a third party service. Other payment systems require movement through multiple channels and systems, outside of the institution's control. For institutions utilizing ACH, and other payment networks, Zelle offers a way to control and manage consumer data. It also facilitates data sharing.

For consumers who use Zelle for transfers between participating banks, the funds are received within minutes. The funds move to a settlement account and are messaged across banks through the Zelle network. The amounts are settled via ACH between banks. For transfers between banks that do not participate in the network, the consumer receives the funds within minutes. The funds are moved to a Visa/MasterCard settlement account, and Zelle communicates between the Zelle participating bank and the non-participating bank. The funds are settled via ACH with Visa/MasterCard.[14]

Zelle's website contains a frequently asked questions section and a user service agreement for consumers. The answers to the questions refer consumers to their bank or credit union for error resolution and timing of fund delivery. The user service agreement available on Zelle's website also warns consumers to only send money to friends and family. The consumer must provide a U.S. address, mobile phone number, and U.S. personal checking or savings account. The consumer's financial institution must permit electronic funds transfers to and from the account. The consumer is not permitted to enroll a prepaid debit card by a financial institution that is not within the Zelle network. The user must also consent to sharing of personal information to institutions within the Zelle network. The shared information includes information necessary to complete the transfer such as verification of a bank account or debit card. The information may be used to comply with fraud prevention inquiries and audits. The consumer must consent to sharing information with institutions as they join the Zelle network.

Zelle's agreement also indicates that the consumer cannot stop a transfer once initiated. According to the agreement, neither Zelle nor the participating network financial institution is

[14] Riveland, Ryan, "Zelle in a Nutshell: Another Faster Payment Option," *NACHA*, 2018.

liable for transfers for (1) any failure to complete a transaction amount, through no fault of Zelle or the institution, or (2) any related losses or damages. The user is solely responsible for ensuring that the correct mobile phone number or email address of the recipient is accurate. This was a recurring point of concern amongst consumers, and reported in various news publications. Consumers reported entering an incorrect phone number or email, and accidentally sending funds to the wrong person. The consumer is unable to retrieve the funds from the incorrect sender because they entered the contact information. Consumers have reported using Zelle to pay for goods and services, but they were unable to initiate any recourse when the good or service was not delivered.[15] Regulation E does not contain servicer or institution requirements for situations where the consumer enters the wrong recipient information.

For consumers sending money between banks in the Zelle network, a consumer cannot cancel a transfer once it is initiated. The funds are immediately transferred. The network banks provide disclosures to the consumer that once the transfer is initiated, it cannot be canceled or recalled. According to the Zelle website, a consumer may only cancel a payment if the recipient has not setup a Zelle account.[16]

For consumers with an account from a non-participating bank, Zelle adheres to the requirements of Section 1005.14 of Regulation E.

> *Section 1005.14(a)(1) states that a person that provides an electronic fund transfer service to a consumer, but does not hold the consumer's account is subject to all requirements if the person issues a debit card (or access device) that the consumer can use to access the consumer's account held by a financial institution, and has no agreement with the account-holding institution regarding such access.*

[15] Cowley, Stacy, "Zelle, the Banks' Answer to Venmo, Proves Vulnerable to Fraud," *New York Times,* 2018.
[16] Early Warning Services, 2018.

The interpretation further states that the section applies only when a service provider issues an access device to a consumer for initiating transfers to or from the consumer's account at a financial institution and the two entities have no agreement regarding this electronic fund transfer service. For situations where the consumer has an account with a bank that does not participate in the Zelle network, Zelle is responsible for complying with the requirements of Regulation E. The Zelle password is also considered an "access device" under Regulation E. Under Regulation E, an "access device" is a card, code, or other means of access to a consumer's account, or any combination thereof, that may be used by the consumer to initiate electronic fund transfers. Consumers use their Zelle password to access the account and transfer funds. Zelle does not have an agreement with the non-participating banks. Thus, Zelle must comply with Regulation E's liability and error resolution requirements for those consumers.

Zelle limits the amount of money to be transferred to $500 per week for consumers connecting accounts to institutions not within the network. Zelle and the institution may change the capped amount. The agreement also directs that if a consumer does not receive the transfer, they should first contact the sender to resolve the issue. Thereafter, any questions about transfers that the consumer initiated using Zelle should go to Zelle first, and then to the financial institution that holds the consumer's account. For errors, the website directs the consumer to contact Zelle by phone, e-mail, or mail no later than 90 days after the consumer received the statement or receipt upon which the problem or error appeared. The notification from the consumer must include the email address or phone number enrolled with Zelle, the type of error and explanation, and the dollar amount. Zelle will review the database of information to determine whether an error occurred. If Zelle determines that an error occurred in the database,

or in the transaction delivery, they will promptly correct the error. If Zelle determines that an error did not occur from the database, Zelle will work with the financial institution that initiated the transfer to assist in the investigation. Zelle will complete error resolution within ten business days and correct the error promptly, alerting the consumer of the results within three business days of completing the investigation. This verbiage is compliant with Section 1005.14 of Regulation E; however, it is unclear as to whether Zelle has a compliance management system in place to monitor and ensure compliance.

Zelle's agreement instructs consumers to contact their financial institution if they believe an unauthorized transfer occurred. For consumers with accounts at institutions that do not participate in the Zelle network, Zelle requires the consumer to report the loss of their Zelle password within four business days after learning of theft or loss to ensure that liability does not exceed $50. Failure to report the password loss within four business days increases liability to $500. This language is compliant with Section 1005.14 of Regulation E. The same liability language is not included for consumers with accounts within the Zelle network because consumers may only access Zelle using their institution's website or mobile app.

The Bureau's EFTA procedures fail to appropriately capture relevant questions for interacting with and assessing Zelle. The EFTA procedures include requirements for disclosures, error resolution, overdraft services, access device issuance, receipts and periodic statements, and gift cards. Of those sections, the disclosures and error resolution sections are applicable to reviewing Zelle. They provide the basic requirements for compliance with Regulation E. However, they fail to clarify expectations for third parties, like Early Warning Service's Zelle. The EFTA procedures also include a paragraph describing the requirements of Section 1005.14,

but do not include specific questions or steps for examiners. The EFTA checklist at the end of the examination procedures also fails to include questions for reviewing Section 1005.14. Examiners may defer to the error resolution and liability sections of the procedures for a basic understanding. However, those requirements are not specific to non-depository providers.

The Bureau's CMS procedures may be used to assess Zelle as a service to participating network banks. The CMS procedures include expectations for developing and maintaining a program that ensures compliance. The components are board and management oversight, policies and procedures, training, compliance monitoring and/or audit, and consumer complaint response. The procedures instruct examiners on how to review these components, and identify strengths and weaknesses. Although the procedures do not contain statutory requirements, examiners may apply the procedure questions in understanding how institutions manage their relationship with Zelle, and how Early Warning Service's manages its compliance expectations for Zelle. The answers to those questions will determine the effectiveness of Regulation E compliance management.

In addition to the CMS procedures, examiners may use the Bureau's service provider oversight bulletin. The bulletin was released on April 13, 2012, and provides expectations in how institutions should oversee their relationships with service providers. Institutions are expected to review and monitor their service providers to ensure that they are in compliance with Federal consumer financial laws and regulations. For examiners reviewing network participating banks, this bulletin serves as a guide for service provider expectations. Specifically, since Zelle is providing a service, institutions that have agreements with Zelle should have policies and

procedures in place for ensuring compliance with Regulation E, and identifying possible unfair, deceptive, or abusive acts or practices.

An assessment of the service provider oversight for each bank is an important component when scoping deposit exams at institutions. Each bank has different expectations and disclosures for the Zelle service. The Zelle network has over one hundred participating banks.[17] Each bank offers a variation of consumer liability and error resolution rights on their public website. As such, the agreements between Zelle and each bank may differ.

In addition to updates to the Bureau's EFTA examination procedures, the FFIEC's Retail Payment Systems procedures require an update. The procedures provide an overview of types of payments and how consumers interact with them. The procedures state that financial institutions should be ready to review and assess emerging payment technologies prior to implementation. They indicate that new payment services should be vetted by risk management to determine the impact; however, the procedures do not provide guidance to examiners on how to assess compliance, or the applicable laws and regulations.

FFIEC Exam Procedures

The FFIEC E-Banking procedures guide examiners in identifying risks associated with E-banking activities. The procedures were last updated in August 2003. They define E-banking as the automated delivery of banking products and services through electronic and interactive channels. E-banking uses computers, mobile phones, and ATMs.

[17] American Bankers Association, 2018.

The procedures guide examiners in reviewing informational and transactional websites. For informational websites, examiners should review accuracy of information, access to confidential information, potential liability for spreading viruses, and negative public perception if the services are disrupted. For transactional websites, where consumers can conduct the transaction, examiners should review safeguarding of customer information, the authentication processes to verify identity, liability for unauthorized transactions, losses from fraud, violations of privacy, content, timing or delivery of disclosures, and negative public perception resulting from failure to process payments, lack of online services, or unauthorized access to consumer information. When assessing Zelle's services and its website, examiners may use the E-Banking procedures to identify possible areas of risk to the consumer.

The E-Banking procedures contain a section on electronic P2P payments. The procedures, however, only reference payments funded through credit card charges or an ACH transfer. They direct examiners to review for potential liability for late payments, liability for payment instructions originating from someone other than the depositor, losses from P2P payments funded from credit cards or accounts where the payee does not have authority, losses from employee misappropriation of funds, and potential liability directing payment availability information to the wrong e-mail recipient. As Zelle users have complained about sending information to the wrong recipient e-mail, examiners may use the procedures to understand the risks faced by Zelle and participating banks.

Since the E-banking procedures serve to guide examiners across agencies, they contain a section on legal and compliance risk. The section includes challenges on uncertainty over legal jurisdiction, disclosure delivery, record retention, and establishment of binding electronic

agreements. The procedures do not reference specific requirements of Regulation E. They instead direct examiners to evaluate the institution's compliance management system, and strategy for E-banking.

Areas where the Bureau has taken action

Prior public actions against payment processors indicate how Zelle may be treated. In March 2016, the Bureau took action against Dwolla, an online payment platform. The Bureau ordered Dwolla to pay a $100,000 penalty and to fix its security practices for deceiving consumers about its data security. The Bureau found that Dwolla failed to employ reasonable and appropriate measures to protect data, and failed to encrypt some sensitive consumer personal information, and released applications to the public before testing.[18] In assessing Zelle, examiners may review data security practices. Banks have reported difficulty in ensuring data protection for faster payments, especially in cases of fraud.[19]

In February 2017, the Bureau took action against Mastercard and UniRush for failing to ensure that consumers had access to their own money. In October 2015, Mastercard and UniRush experienced multiple failures, causing consumers to be unable to use their paychecks and other direct deposits for cash withdrawals, bill pay, or to obtain balance information. UniRush failed to provide customer service. The Bureau ordered Mastercard and UniRush to pay $10 million in

[18] (Bureau of Consumer Financial Protection, 2018) Bureau of Consumer Financial Protection, "CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices," *Bureau of Consumer Financial Protection,* 2018, https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/ (Accessed December 4, 2018).
[19] Hernandez, Will, "Is fear of fraud holding back faster payments?," *American Banker*, 2018.

restitution to tens of thousands of harmed consumers. The Bureau also fined Mastercard and UniRush $3 million.

UniRush LLC is the program manager for RushCard, a reloadable prepaid debit card. Mastercard Payment Transaction Services is the payment processor for the RushCard. RushCard is advertised as a way for consumers to receive direct deposits on their card "up to two days sooner." These deposits include government benefits or payroll funds. In 2014, UniRush picked Mastercard as its new payment processor. UniRush switched to Mastercard's processing platform in October 2015. At the time of the switch, RushCard had about 650,000 active users, of which about 270,000 received direct deposits on their RushCard.

The Bureau found that Mastercard or UniRush denied consumers access to their own money by not accurately transferring all accounts to Mastercard. As a result, thousands of consumers could not access funds stored on their cards for days or weeks. About 1,110 consumer accounts were incorrectly suspended. UniRush also delayed crediting cash deposits to consumers' accounts and shut off access to certain funds that consumers put aside for savings. UniRush did not issue a working replacement card to consumers whose cards were lost or stolen during this period. UniRush delayed processing direct deposits for more than 45,000 consumers, and did not process or improperly returned deposits for 2,000 other consumers. As a result, consumers could not access their paychecks or government benefits. UniRush also erroneously double posted deposits and did not promptly process electronic debit transactions, which falsely inflated those RushCard holders' account balances. Thousands of consumers accidentally spent more money than was loaded on their RushCard. With no advance notice to consumers, UniRush used funds consumers subsequently loaded onto their RushCards to offset negative balances caused by its

processing errors. Mastercard did not make sure it was sending accurate information about consumers' account balances to UniRush when it declined to authorize certain transactions. As a result, some consumers received incorrect information telling them their account balances were zero, when the consumers actually had funds stored on their cards. UniRush did not have an adequate plan to step up its customer service response to meet the increased demand caused by service disruptions. Even after hiring additional personnel, UniRush failed to train customer service agents in time to meet the surge in demand. As a result, some consumers who called customer service waited on hold for hours and could not obtain critical information about the status of their funds and accounts.[20] In reviewing Zelle's practices, examiners may direct their focus on understanding possible unfair or deceptive practices, where consumers do not have access to funds, or when account balances are not accurately updated.

In June 2016, the Bureau filed a suit against payment processor Intercept Corporation for allegedly enabling unauthorized and other illegal withdrawals from consumer accounts by their clients. Intercept Corporation is a third-party payment processor located in Fargo, N.D. Intercept transmits electronic funds transfers through ACH on behalf of its clients. Intercept's clients include payday lenders, auto-title lenders, debt collectors and sales financing companies. The Bureau alleged that Intercept processed payments for clients without adequately investigating, monitoring, or responding to red flags that indicated some clients were breaking the law or deceiving customers. Intercept allegedly ignored blatant warning signs of potential fraud. High

[20] (Bureau of Consumer Financial Protection, 2018) Bureau of Consumer Financial Protection, "CFPB Orders Mastercard and UniRush to Pay $13 Million for RushCard Breakdowns That Cut Off Consumers' Access to Funds," *Bureau of Consumer Financial Protection*, 2018, https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-mastercard-and-unirush-pay-13-million-rushcard-breakdowns-cut-consumers-access-funds/ (Accessed December 4, 2018).

rates of returned payments for insufficient funds or unauthorized debits may indicate that consumers did not consent to the withdrawal or were misled about the terms. Many of Intercept's clients have annual return rates of 20 to 40 percent for network transactions, far above the 1.5 percent industry average. Intercept made little effort to find the cause of these rates, and, despite the red flags, kept processing transactions for these clients. Intercept allegedly ignored complaints and warnings from banks and consumers about high return rates and initiating unauthorized debits, including for payday lenders in states where the practice is illegal. On at least one occasion, Intercept entered into a trial period with a financial institution to process a limited number of payments, but then ran millions of dollars of network transactions through the bank, generating high volumes of returns. If banks raised concerns about consumer complaints against an Intercept client, Intercept would simply seek out a new bank to help it process payments for the same clients. Intercept moved between eight different banks between 2008 and 2014. The US District Court dismissed the complaint in March 2017 because the Bureau failed to provide specific factual data verifying the arguments made in the complaint.[21] Although the court dismissed the complaint, the type of arguments presented are possible areas of concern within the UDAAP framework. Zelle is intended to be used for P2P transactions, and should only transfer available funds. Examiners may review the timing of fund transfers, and how Zelle treats repeat transfer requests where funds are not available.

Zelle's Peer

[21] Bureau of Consumer Financial Protection, "Intercept Corporation, d/b/a InterceptEFT, Bryan Smith, and Craig Dresser," *Bureau of Consumer Financial Protection*, 2017, https://www.consumerfinance.gov/policy-compliance/enforcement/actions/intercept-corporation-db-intercepteft-bryan-smith-and-craig-dresser/ (Accessed December 4, 2018).

Venmo is Zelle's largest competitor, with over 140 percent growth between the first quarters of 2015 and 2016.[22] In the third quarter of 2018, PayPal reported $16.7 billion in transactions processed across Venmo. This is a 78 percent increase from third quarter of 2017.[23] Venmo leverages social media, and the ability for consumers to share why and how they are making payments to friends. Venmo requires consumers to wait a few days before receiving funds in their accounts. Venmo also operates on a different model. While Zelle moves money between consumer accounts real-time, Venmo stores transferred funds. Consumers can withdraw from their Venmo balance at any time, but will not immediately receive the funds.

Venmo is not subject to the same requirements as Zelle. Venmo initiates transfers through contacting the associated bank account, and requesting an ACH transfer. Unlike Zelle, consumers make payments using a Venmo balance, or by linking a bank account, debit card, or credit card.[24] The consumer's Venmo balance contains the stored value of funds so that funds available for new transactions are not subject to pending transactions. Venmo will use this balance first, and then cover the remaining using the consumer's bank account, debit card, or credit card. Consumers may not cancel the transfer once requested, and Venmo may resubmit the ACH debit if it is returned with insufficient funds. Debit card and credit card transfers are through the ATM network or the Visa/Mastercard network.

Venmo's user agreement contains language for protecting consumers from unauthorized transactions and other errors. Venmo defines an unauthorized transaction as a situation where an

[22] King, WB, "Can Zelle Trump Venmo in P2P Exchanges? A Group of CU and Banks are Betting on It," *Credit Union Journal*, 2016.
[23] PYMTS, 2018
[24] Venmo, "About Payment Methods," *Venmo*, 2018 https://venmo.com/legal/us-payment-method-rights (Accessed December 4, 2018).

individual steals a password, uses the password to access the account, and sends a payment. However, if the consumer willingly shares the password, and that person sends a payment without the consumer's knowledge or permission, the consumer is responsible. Venmo defines an error as a consumer sending a payment and the debiting or crediting the incorrect amount. An error also includes transactions missing from the account statement, and computational errors by the company. If, however, the consumer loses their mobile phone, which contains login information, and unauthorized transactions occur, Venmo will refund the full amount if the consumer immediately notifies the company. The consumer must notify Venmo within 60 days of the unauthorized transfer or error appearing on the account. Venmo will conduct an investigation, providing provisional credit, and an explanation of findings.

Venmo's requirements under Regulation E differ based on the payment method. Venmo allows consumers to link their bank account, but it also holds funds in their Venmo account. PayPal owns Venmo, and in their annual 2017 10K report, PayPal reported that they are subject to certain requirements of Regulation E, but are still contemplating the extent of those requirements. In October 2016, the Bureau issued the final rule of prepaid accounts. A prepaid account includes accounts that may be loaded, and whose primary function is to conduct transactions with multiple unaffiliated merchants for P2P transfers, including digital wallets. The rules include requirements for disclosures, liability, and error resolution. The Bureau made additional amendments for linking credit cards to digital wallets, and the final rule was issued in January 2018, with an effective date of April 1, 2019. In its 2017 10K, PayPal stated that they are evaluating the applicability of the rule. PayPal has paid amounts to settle allegations of violations

of the EFTA in the past.[25] In 2012, PayPal reached a settlement resulting from a class action lawsuit regarding its dispute resolution process. PayPal agreed to pay $4million to a settlement fund, update its hold disclosures, and clarify its dispute resolution process.[26] Venmo is subject to Section 1005.20 of Regulation E for funds that are stored in the Venmo balance. Section 1005.20 contains requirements for gift cards and gift certificates. However, unlike Zelle, Venmo is not subject to Section 1005.14(a) of Regulation E. Since Venmo links accounts and transfers funds via ACH agreements, this section does not apply. The user experience for both Zelle and Venmo is similar. Examiners should keep in mind the differences between both types of providers, and the consumer impact for each. Examiners can apply the UDAAP principles, and evaluate the compliance management practices for both using similar frameworks.

Zelle's Challenges

Regulators should understand Zelle's challenges and the impact to consumers. Although Zelle advertises quick and easy payments, consumers have complained about the setup process. For consumers without banks that offer Zelle, they need to undergo an additional setup process. This appears to be where issues regarding adopting the technology, and using it, occur. Consumers that do not bank with Zelle affiliated banks need to download the Zelle app, open an account, and link the account to their bank. Zelle puts consumers through multiple authentication processes, which may result in issues setting up the account. During its initial launch, Zelle was only available to consumers that used banks within the network. In September 2017, the reach

[25] PayPal Holdings, Inc., "2018 Annual Meeting of Stockholders and Proxy Statement and 2017 Annual Report," *Security and Exchange Commissions*, 2018.
[26] Maynard, Christopher, "Class action settlement over PayPal account closures finally finds resolution," *Consumer Affairs,* 2017 https://www.consumeraffairs.com/news/class-action-settlement-over-paypal-account-closures-finally-finds-resolution-032817.html (Accessed January 9, 2019).

expanded with the app. For banks that do offer Zelle, P2P has grown. Bank of America processed 68 million Zelle transactions in 2017, an increase of 84 percent from 2016.[27] As of January 2019, Early Warning Services reported 60 institutions on the Zelle network. Bank of America drove most of the transaction volume, with 51.6 million transactions totaling $14 billion in the fourth quarter of 2018.[28] After its launch, Zelle also faced issues with connecting consumer accounts with phone numbers and email addresses. If a consumer had an account through clearXchange with a bank, they had to remove account links if they wanted to choose a different bank.[29]

Zelle also faces issues around fraud. Banks have found that scammers offer to sell items and request payment through Zelle. Consumers are willing to use Zelle because of its association with large banks. The scammers will obtain the funds, and immediately disconnect contact with the consumer. The consumers do not have recourse, as banks have not taken action on these fraudulent transactions. Zelle's website cautions consumers to only make payments to known parties.[30] Examiners may review how consumers are able to file disputes, the timeliness of the filing, and how each bank handles them. Regulation E's stop payment requirements do not apply to the Zelle service. Nonetheless, the requirements around stop payments could serve as a guideline for institutions in developing protections for consumers.

Fraud is also a concern when actors are not actively attempting to cause harm. For example, a consumer may register a phone number and associate it with their account. Since the

[27] Peters, Andy, "Zelle's anti-fraud efforts trip up key group: Its users," *American Bankers,* 2018.
[28] Fitzgerald, Kate, "Zelle's volume surges, but there's a catch," *Payments Source*, 2019.
[29] Holland, Nick, "Zelle signup issues expose risks of tying phone numbers to accounts," *American Banker,* 2017.
[30] Gartenberg, Chaim, "Zelle users are getting scammed just like on Venmo," *The Verge*, 2018.

phone number and account are linked, if their number changes, money may be incorrectly sent to them. In those cases, the sender may not be able to retrieve the money because the correct phone number was entered. The issue was that the consumer associated with the number was different than the intended recipient.[31] Examiners may review how banks update contact information, and ensure accuracy in their data.

Other consumers have reported phishing schemes with Zelle. Fraudsters call the consumer indicating that they are calling from their bank and request the authentication codes texted by the bank. This enables fraudulent account access, and the ability to use Zelle to quickly move funds. Examiners may review fraud protection practices, and how each bank treats unauthorized transactions.

Examiners may assess Zelle's challenges in securing a safe and secure payment system through the Unfair, Deceptive, and Abusive Acts of Practices (UDAAP) examination procedures. Zelle's use of a phone number or email address as the only way to connect to a consumer's account may be unfair. Zelle ties bank accounts to email addresses or phone numbers as "unique identifiers" (not names). The New York Times reported on a consumer who attempted to send funds to his mother using her phone number. The money was sent to a different person who registered the phone number to his account. The bank did not refund the consumer because he entered the phone number, and initiated the transfer. In other cases, the consumer entered the correct recipient name but accidentally transposed the phone number, and the money was sent to the account associated with the phone number. The consumer was not refunded because the phone number was the "unique identifier" for sending money. Zelle does not compare the

[31] Cowley, 2018.

recipient name and number to the accountholder name. Examiners may use the framework within the UDAAP procedures to determine whether this practice is unfair to consumers.

Institutions have also identified fraud as a high area of concern, and have identified ways to mitigate the risk. For instance, in December 2017, PNC Bank started using The Clearing House's real-time payment network. Thus far, transaction volume is low, and PNC has not identified fraud. PNC reviews transactions to determine whether either party is on the Office of Foreign Assets Control list, and to determine if the payment is similar to historical transactions. The Clearing House also screens each transaction to determine if either party has history of fraud. Conversely, institutions that only use Zelle have identified high rates of fraud. Early Warning provides banks with a readiness assessment checklist before going live with the Zelle network. Zelle's participating banks also provide weekly reports to Zelle on fraud. Early Warning anticipates providing consumers with the name of the recipient to avoid sending money to the wrong person.[32]

The Bureau should continue to review and assess P2P payment providers, and areas of consumer harm. In understanding the product and processes, the Bureau can determine the appropriate and applicable regulatory requirements. The Bureau should then take steps to update

[32] Crosman, Penny, "How Zelle, banks combat real-time payment fraud," *American Banker,* 2018.

examination procedures and checklists so that examiners can accurately apply the regulatory requirements.

Part IV: Recommendations

Methods in Providing Guidance on P2P Payments

Vision of Consumer Protection in New Faster Payment Systems

One way for the Bureau to better understand and assess Zelle is through its 2015 Vision of Consumer Protection in New Faster Payment Systems. The vision principles outline expectations for a safe, transparent, accessible, and efficient payment system that includes consumer protection concerns. The principles may be applied to how regulators think about Zelle in the following way:

1. Consumer Control Over Payments

Examiners should understand how much control consumers have over their money. This includes reviewing how financial institutions disclose when, how, and under what terms consumers have authorized a transfer. Examiners should review whether the system enables the consumer to place parameters on the payment, including a time period, amount, and transferee. The system should also have procedures enabling the consumer to revoke the authorization for the transfer. Examiners may assess the level of control consumers have over sending funds, especially the ability to cancel and identify the recipient.

2. Data and Privacy

Examiners should review how institutions maintain personally identifiable information. Financial institutions should inform consumers on how their data is transferred through the Zelle network,

and what data is transferred. Since Zelle is the result of multiple banks collaborating for faster payments, consumers should be aware of the data shared in the partnership and potential risks. When consumer data is collected, it should be used in ways that benefit consumers. The system should protect against misuse of the data associated with payment transactions. For instance, Early Warning receives weekly fraud reports from participating institutions. Examiners may assess how this information is used and disseminated.

3. Fraud and Error Resolution Protections

Examiners should understand how data is retained, and the error resolution process. Examiners should determine whether Early Warning has the system architecture creates and records post-transaction evaluation. The system should provide mechanisms for reversing erroneous and unauthorized transactions quickly once identified. It should also provide consumers with regulatory protections, such as Regulation E and Regulation Z, along with other appropriate safeguards.

4. Transparency

Examiners should review how much information Zelle provides to consumers. Examiners should determine whether Zelle provides real-time access to information about the status of transactions, including confirmations of payment and receipt of funds. Consumers should also receive timely disclosure of the costs, risks, funds availability, and security of payments. If funds are unavailable, or need to be re-authorized, consumers should be able to review their account balance, and be assured of its accuracy.

5. Cost

Examiners should review how costs of the service are disclosed. Examiners should review how Zelle ensures that fees are disclosed to consumers, and that pyramiding of fees, or other areas where the consumer is charged exorbitant fees do not occur. Fees charged to consumers are disclosed in a manner that allows consumers to compare the costs of using different available payment options. For consumers using any system, fee structures do not obscure the full cost of making or receiving a payment.

6. Access

Examiners should review how broadly Zelle and other payment services are accessible to consumers. To ensure access and usability, systems are widely accepted by businesses and other consumers. They permit consumer access through qualified intermediaries and other non-depositories, such as mobile wallet providers and payment processors, except to the extent necessary to protect functionality, security, or other key values.

7. Funds Availability

Examiners should determine whether consumers have access to their money. This includes determining guaranteed access to funds, which decreases consumer risk of overdraft and declined transactions due to insufficient funds. Consumers should be made aware of when funds are transferred and received, and have access to the most up-to-date account balance information.

8. Security and Payment Credential Value

Examiners should review the security of consumer payments. Examiners should determine if Zelle has built-in protections to detect and limit errors, unauthorized transactions, and fraud. It should also limit the value of consumer payment credentials so that security breaches are of limited worth to fraudsters. Zelle holds unique identifier information for consumers. Zelle should

ensure that the data and is maintained in a secure manner, and that they have a plan in the case of a security breach.

9. Strong Accountability Mechanisms that Effectively Curtail System Misuse

Examiners should review Zelle's ability to curtail misuse. Zelle's participants should be accountable for risk, harm, and costs. They should be incentivized to prevent and correct fraudulent or unauthorized transactions. Zelle should have automated monitoring, and incentives for reporting misuse. Since Zelle is a collaborative effort across large depository institutions, it should have mechanisms for reporting misuse across the network.

Consumer Protection Principles for Consumer-Authorized Financial Data Sharing and Aggregation

In October 2017, the Bureau also issued Consumer Protection Principles for Consumer-Authorized Financial Data Sharing and Aggregation. Data aggregation services include financial management tools, verification of accounts and transactions, facilitation of underwriting or fraud-screening, and other functions. The Bureau released principles intending to emphasize the importance of consumer interests in services that use consumer-authorized financial data. The principles expressed the vision of a robust, safe, and workable data aggregation market. Zelle's platform enables information sharing across institutions. The Bureau may use these principles as best practices for reviewing Zelle's services in the following way:

1. Access

Consumers should be able to obtain information about their ownership or use of a product or service from the provider. The information should be made available timely, and the information

should be held in a safe manner. The account agreements should support safe, consumer-authorized access, promote consumer interests, and do not deter consumers from accessing their information. Access should not require the consumer to share account credentials with third parties. For institutions that participate in the Zelle network, consumers are able to use the service through their mobile app.

2. Data Scope and Usability

Consumers should be aware of the amount of accessible data. Financial data subject to consumer and consumer-authorized access may include any transaction, series of transactions, or other consumer usage. Information should be available in forms that are readily usable by consumers and consumer-authorized third parties. Third parties with authorized access should only access the data necessary to provide the product or service. The information provided for the Zelle platform is not publicly available. Zelle, however, advertises safe and secure payments. Information about consumer accounts that is shared across the platform should be limited.

3. Control and Informed Consent

Consumers should control information regarding their accounts and use of financial services. Zelle should effectively disclose the terms of access, storage, use, and disposal of data. The disclosures should be understandable and consistent with the consumer's expectations. Consumers should not be coerced into granting third-party access, and should be able to readily revoke access. It is unclear what, and how much information, is maintained by Zelle after the consumer revokes access to their account. It is also unclear as to whether Zelle reports any information to consumer reporting agencies.

4. Authorizing Payments

Zelle should obtain separate and distinct consumer authorizations for data access and payment authorization. By enrolling in Zelle, consumers provide access to data. This authorization should differ from the payment authorization for each transaction.

5. Security

Consumer data should be accessed, stored, used, and distributed securely. Data should be maintained in a format that protects against security breaches. As the Zelle platform moves information across institutions, the type of information stored should be maintained in a secure environment. The information sharing across institutions to Zelle, such as fraud reports, should be submitted in a secure manner.

6. Access Transparency

Consumers should be informed of which third parties are authorized to access or use their information. The identity and security of each party, the data they access, their use of the data and the frequency of access should be ascertainable by the consumer.

7. Accuracy

Data should be accurate and current. Consumers should have a reasonable means to dispute and resolve data inaccuracies. As Zelle uses unique identifiers attached to accounts, consumers should be able to correct any inaccuracies with the identifiers. Zelle should disclose how a consumer can correct inaccuracies via Zelle or their depository institution.

8. Ability to Dispute and Resolve Unauthorized Access

Consumers should have reasonable and practical means to dispute and resolve instances of unauthorized access and data sharing, unauthorized payments conducted in connection with, or as a result of data access, and failures to comply with other obligations. Consumers are not required to identify the party who gained or enabled unauthorized access in order to receive appropriate remediation.

9. Efficient and Effective Accountability Mechanisms

The goals and incentives of parties that grant access to, access, use, store, redistribute, and dispose of consumer data should align to enable sage consumer access and deter misuse. Commercial participants should be held accountable for misuse. They should also be incentivized to prevent, detect, and resolve unauthorized access and data sharing, and unauthorized payments.

In addition to using the Bureau's vision and principles, examiners should understand the intent of the EFTA, and how it applies to P2P payments. An update to the examination procedures, to include Zelle and other payment services, is important because of growth and impact in the P2P payment market. Examiners need to be equipped with tools that contemplate the use of P2P payments, and how to determine applicability of the regulations.

The Bureau can begin reviewing EFTA procedures for applicability, and develop further questions regarding payment processing. For instance, Section II – Subpart A of the procedures contains guiding questions for transaction testing, policies and procedures, and disclosures. The section updates may include determining whether the service provider issues a debit card or other access device that the consumer can use to access the account, and if the provider has an

agreement with the account-holding institution regarding such access. The answer to those questions will determine the Regulation E requirements for the provider. Once examiners are able to make that determination, they can choose which sections of the procedures are applicable. If the service is similar to Zelle, examiners will need to review for compliance with the appropriate subsection.

The Bureau may also issue guidance to examiners and financial institutions for contemplating how the UDAAP framework applies to P2P services. This includes applying the framework to advertisements, enrollment, processing of transactions, disputes, and requests to end the service. The UDAAP framework, and the Bureau's prior opinions on what constitutes UDAAP offer ways to assess the consumer impact. By using the tools available, such as the EFTA procedures, the CMS procedures, the FFIEC procedures, and public guidance, the Bureau can begin reviewing and updating examination procedures.

As the payment market and systems continue to evolve and progress, the Bureau needs to expand the use of current guidelines and framework to appropriately capture areas of consumer risk. The tools at examiner disposal, including exam procedures, bulletins, and findings on public enforcement actions, serve to direct examiners to possible areas of risk, and how prior actions may dictate future responses. Those tools, although useful in setting expectations, do not provide sufficient guidance. In order to ensure that examiners have appropriate tools, the Bureau should update examination procedures and training. By updating the examination procedures to include all of the EFTA requirements, Bureau examiners will have access to materials that can be applied to Zelle, and other advancements in the P2P market. This will drive consistency in how examiners view the product at different institutions, and how similar products are evaluated.

Other regulators that examine institutions not within the CFPB's jurisdiction can also leverage these procedures. Procedure updates will serve as a signal to the financial marketplace that regulators are nimble, and ready to review and understand how these products work, and the impact on the consumer.

Bibliography

American Bankers Association. (2018). *Understanding Zelle*. Retrieved from ABA: https://www.aba.com/Tools/Function/Technology/Documents/UnderstandingZelle.pdf

Board of Governors of the Federal Reserve System. (2016). *The Federal Reserve Policy on Payment System Risk.* Washington: Board of Governors.

Bradford, T., & Keeton, W. (2012). *New Person-to-Person Payment Methods: Have Checks Met Their Match?* Kansas City: Federal Reseve Bank of Kansas City.

Bureau of Consumer Financial Protection. (2017, October 18). *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation.* Retrieved from consumerfinance.gov: https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf

Bureau of Consumer Financial Protection. (2017, March 17). *Intercept Corporation, d/b/a InterceptEFT, Bryan Smith, and Craig Dresser .* Retrieved from Bureau of Consumer Financial Protection: https://www.consumerfinance.gov/policy-compliance/enforcement/actions/intercept-corporation-db-intercepteft-bryan-smith-and-craig-dresser/

Bureau of Consumer Financial Protection. (2018, February 1). *CFPB Orders Mastercard and UniRush to Pay $13 Million for RushCard Breakdowns That Cut Off Consumers' Access to Funds.* Retrieved from Consumer Financial Protection Bureau: https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-mastercard-and-unirush-pay-13-million-rushcard-breakdowns-cut-consumers-access-funds/

Bureau of Consumer Financial Protection. (2018, March 2). *CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices.* Retrieved from consumerfinance.gov: https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/

Clark, D. (2018, June 13). *Zelle to OVertake Venmo in 2018.* Retrieved from eMarketer: https://www.emarketer.com/newsroom/index.php/zelle-to-overtake-venmo-in-2018/

Cowley, S. (2018, April 22). Zelle, the Banks' Answer to Venmo, Proves Vulnerable to Fraud. *New York Times*. Retrieved from https://www.nytimes.com/2018/04/22/business/zelle-banks-fraud.html

Crosman, P. (2018, October 10). How Zelle, banks combat real-time payment fraud. *American Banker*.

Early Warning Services, LLC. (2018, October 19). *Frequently Asked Questions.* Retrieved from Zelle: https://www.zellepay.com/support/can-i-cancel-a-payment

Early Warning Services, LLC. (2018, October 19). *Just in Time Notice for Zelle App.* Retrieved from Zelle: https://www.zellepay.com/just-time-notice

Early Warning Services, LLC. (2019, January 24). *Zelle® Ends 2018 with its Strongest Quarter on Record.* Retrieved from ZellePay: https://www.zellepay.com/press-releases/zelle-ends-2018-its-strongest-quarter-record

Early Warning Services, LLC. (2019, January 24). *Zelle® Ends 2018 with its Strongest Quarter on Record.* Retrieved from zellepay.com: https://www.zellepay.com/press-releases/zelle-ends-2018-its-strongest-quarter-record

FFIEC. (2016). *Retail Payment Systems Handbook.* Washington, DC: FFIEC.

Fitzgerald, K. (2019, January 24). Zelle's volume surges, but there's a catch. *Payments Source*. Retrieved from https://www.paymentssource.com/news/zelles-volume-surges-but-theres-a-catch

Gartenberg, C. (2018, February 16). Zelle users are getting scammed just like on Venmo. *The Verge*.

Hernandez, W. (2018, November 28). Is fear of fraud holding back faster payments? *American Banker*. Retrieved from https://www.americanbanker.com/news/is-fear-of-fraud-holding-back-faster-payments?utm_campaign=daily%20briefing-nov%2029%202018&utm_medium=email&utm_source=newsletter&eid=5987ea3588a847bd9b3e49006fc4a643&bxid=52b26dd4c16bcfa46fef20ee

Holland, N. (2017, July 10). Zelle signup issues expose risks of tying phone numbers to accounts. *American Banker, 182*(130), 1.

King, W. (2016, December 12). Can Zelle Trump Venmo in P2P Exchanges? A Group of CU and Banks are Betting on It. *Credit Union Journal, XX*(25), 10.

Maynard, C. (2017, March 28). *Class action settlement over PayPal account closures finally finds resolution.* Retrieved from Consumer Affairs: https://www.consumeraffairs.com/news/class-action-settlement-over-paypal-account-closures-finally-finds-resolution-032817.html

PayPal Holdings, Inc. (2018). *2018 Annual Meeting of Stockholders and Proxy Statement and 2017 Annual Report.* Washington, DC: Securities and Exchange Commission.

Peters, A. (2018, January 18). Zelle's anti-fraud efforts trip up key group: Its users. *American Banker, 183*(12), 1.

PYMNTS. (2018, October 19). *PayPal Posts 25 Pct Jump In Payments Volume.* Retrieved from PYMNTS: https://www.pymnts.com/earnings/2018/paypal-stocks-payments-transaction-volume/

Riveland, R. (2018). *Zelle in a Nutshell: Another Faster Payment Option.* NACHA. Retrieved from https://web.nacha.org/system/files/resource/2018-02/Zelle%20webinar%20presentation%201.30.18.pdf

Venmo. (2018, October 10). *About Payment Methods*. Retrieved from Venmo: https://venmo.com/legal/us-payment-method-rights

Wolfe, D. (2018, September 24). Zelle no! Credit unions balk at joining bank-run P2P network. *Payments Source*. Retrieved from https://www.paymentssource.com/news/credit-unions-balk-at-joining-zelle-p2p