University of Michigan Journal of Law Reform

Volume 57

2024

It Takes a Thief…. and a Bank: Protecting Consumers from Fraud and Scams on P2P Payment Platforms

Cathy Lesser Mansfield
Case Western Reserve University School of Law

https://doi.org/10.36646/mjlr.57.2.takes

IT TAKES A THIEF . . . AND A BANK: PROTECTING CONSUMERS FROM FRAUD AND SCAMS ON P2P PAYMENT PLATFORMS

Cathy Lesser Mansfield*

ABSTRACT

This Article proposes statutory and regulatory changes to the Electronic Fund Transfer Act; Regulation E; and the Bank Secrecy Act/Anti-Money Laundering regulations to protect consumers who use instant payment platforms in the United States (such as Zelle and Venmo) from scam artists and fraudsters. After discussing current fraud scams on these payment platforms, the Article discusses the history and context of the 1978 Electronic Fund Transfer Act and Regulation E, and the definition of unauthorized payments and payments made in error therein. The second part of this Article explores changes to the Bank Secrecy Act/Anti-Money Laundering regulations that might make it hard for fraudsters to use the financial system to commit fraud, and might make it easier for financial institutions to identify fraudsters seeking to do so. Finally, this Article provides an update on regulatory, legislative, and judicial activity that took place while this Article was in the process of being published.

TABLE OF CONTENTS

* Cathy Lesser Mansfield is on the faculty at Case Western Reserve University School of Law, where she teaches commercial and consumer law courses. Previously, she was a Professor of Law at Drake University School of Law and a Visiting Professor of Law at Georgetown University Law Center. She served as a policy analyst at the Consumer Financial Protection Bureau for two years; is an author on the National Consumer Law Center's Consumer Banking and Payments Law manual; and represents the National Consumer Law Center on the Board of Directors of the Faster Payments Council.

I. INTRODUCTION

Consumers who use Peer-to-Peer (P2P)/Peer-to-Business (P2B) (hereinafter collectively called P2P) payment platforms in the United States (such as Zelle and Venmo) need better legal protection from scam artists and fraudsters. This Article proposes statutory and regulatory changes that would place the loss for P2P payments induced by fraud on the financial institutions that own and operate P2P payment platforms, rather than on consumers. It also lays out the policy justifications for placing these losses on financial institutions—particularly those that provide bank accounts to fraudsters. Without these guardrails, it is too easy for fraudsters to take the money and run, and consumers may become justifiably wary of a payment system that otherwise provides immense convenience and ease of use.

The statutory and regulatory changes proposed in this Article should and can be made: by Congress, through amendments to the Electronic Fund Transfer Act (EFTA), by the Consumer Financial Protection Bureau, through amendments to Regulation E, and by the Financial Crimes Enforcement Network, through changes to the Bank Secrecy Act/Anti-Money Laundering regulations. These changes to the law will protect victims of fraud and scams on P2P payment platforms, bring the rules governing loss from electronic payments fraud into the

twenty-first century, and incentivize financial institutions to protect the U.S. financial system and consumers from fraudsters and scam artists who use P2P platforms to ply their trade.[1]

II. UNDERSTANDING PAYMENTS FRAUD SCHEMES: THE PROBLEM

A. *Introduction to the Problem*

There are many different fraudulent schemes that rely on the characteristics of a particular payment system to help the perpetrator succeed in the fraud and abscond with the payment. Over the years, fraud schemes have been inconsistently categorized: sometimes by type of fraud or perpetrator, sometimes by payment system used, and sometimes by some other criteria. Lack of consistency in identifying and categorizing types of payment fraud led the Federal Reserve to adopt the "FraudClassifier Model" in June 2020, which identifies and classifies fraud based on the type of fraud used, rather than by the payment system used.[2] This Article focuses on one type of payments fraud, identified in the FraudClassifier Model as payments initiated by an "authorized party" who has been manipulated, as perpetrated in one type of payments system—P2P payments platforms.[3]

---

1. It should be noted that some of the proposals in this Article, in particular the section on BSA/AML, could also help protect businesses from fraud as well.

2. Press Release, Bd. of Governors of the Fed. Reserve Sys., Federal Reserve Announces FraudClassifier Model to Help Organizations Classify Fraud Involving Payments (June 18, 2020).

3. The FraudClassifier Model classifications can be seen at https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/, and an interactive model can been seen at https://fedpaymentsimprovement.org/fraudclassifier/index.html. The "manipulation" category of payments fraud is further broken down in two sub-categories: Products and Services Fraud, and Relationship and Trust Fraud. FraudClassifier Interactive Model, available at https://fedpaymentsimprovement.org/fraudclassifier/index.html. The example given for Products and Services Fraud in the FraudClassifier Model is:

> Scenario: In addition to his recurring condo fee payments, Paul received an invoice for planned roofing repairs that appeared to be from his condo association. Paul sent a check to the address on the invoice. Soon after, he reached out to the condo association only to be told that the roof had just been replaced a couple of years ago and they had never sent an invoice.
>
> Explanation: Paul paid the invoice with his money (or from his account). He did so believing he was paying for a roof repair to his condo when in actuality, no roof repair was conducted and the invoice he received was fake/fraudulent. FraudClassifier Interactive Model, available at https://fedpaymentsimprovement.org/fraudclassifier/index.html.

The example given for Relationship and Trust Fraud in the FraudClassifier Model is:

> Scenario: Joan fell in love with Fred via an online dating site. They decided to meet in person. A day before meeting, Fred asked Joan to wire him $10,000 to get out of serious trouble.

Over the years, the methods of payment have evolved from a system dependent on cash and checks to a system that increasingly uses electronic processing of payments, including credit cards, debit cards, automatic account withdrawals, online bill paying, and wires.[4] In recent years, consumers have been given access to payment systems that allow them to make direct, real time payments to other individuals (P2P payments) and to businesses (P2Bpayments).[5] Examples of these services are Zelle, Venmo, and CashApp. These services move money in near real time, and do not enable the sender (or, in the case of Zelle, the sender's institution) to recall funds.[6] It is for these reasons that these services have become the "preferred tool for grifters."[7]

Imagine you are a fraudster, and you want to steal money by inducing unwary individuals and small businesses to make payments to you to which you are not entitled. In addition to figuring out how to deceive your victims into initiating a payment to you, you must decide what payment system you will ask your victims to use, and what system you will use if your scam involves sending phony money to your victim. Will you use cash? Checks? Certified checks? Electronic payments through the Automated Clearing House (ACH) network? If you are smart, you pick the payment system that processes the payments to you in the fastest way possible—before your victims, or their family and friends, find out about what you have done and stop the payment before it is complete.[8] Today, the fastest payment system available is the P2P system. If you use the P2P

Joan wired the money to Fred. The next day, Fred did not show up for their date as planned. Joan made several attempts to reach out to Fred but never heard from him again.
Explanation: Joan gave Fred money from her account. She was manipulated by Fred to send the money via Fred's guise of beginning a romantic relationship. FraudClassifier Interactive Model, available at https://fedpaymentsimprovement.org/fraudclassifier/index.html.

4. *Federal Reserve Payment Study (FRPS)*, BD. GOVERNORS FED. RESERVE SYS. (Apr. 21, 2023), https://www.federalreserve.gov/paymentsystems/frps_previous.htm [https://perma.cc/RT4Z-DFSK] (studying approximately every two years to report payment methods used in the U.S. economy showing a decreased use of cash and checks and increased use of electronic payments).

5. In this Article, collectively called P2P.

6. Paige Pidano & Tara Payne, *Fraud on P2P Payment Apps Like Zelle and Venmo: A Primer*, BANK POLICY INSTITUTE (Feb. 23, 2022), https://bpi.com/fraud-on-p2p-payment-apps-like-zelle-and-venmo-a-primer/ [https://perma.cc/JN2S-8QYV] ("[M]oney sent on P2P platforms should be thought of like cash: Accessible instantly, or close to it, and difficult to recover if it's sent to someone by mistake.").

7. Stacy Cowley & Lananh Nguyen, *Fraud is Flourishing on Zelle. The Banks Say It's not Their Problem*, N.Y. TIMES (Mar. 6, 2022), https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html [https://perma.cc/DV9W-URD7].

8. *See* Jon Healey, *Do You Use Zelle? Here's How to Spot Increasingly Common Scams*, L.A. TIMES: TECH. & INTERNET (Oct. 7, 2022, 4:00 AM), https://www.latimes.com/business/technology/story/2022-10-07/zelle-banks-may-not-cover-the-losses-from-scams [https://perma.cc/L5C9-F77T] (commenting that Zelle is attractive to fraudsters for precisely this reason).

system to receive payment from your victim, your entanglements with the banking system (at least as far as that payment is concerned) end once you are paid. No bank will need to come after you for the money because the payment will always go through. The fraudster's bank will never have to face a returned payment, and so the fraudster's bank will never seek to charge back against the fraudster.

B. *Manipulation Fraud Schemes Involving Payments*

Payments fraud involving manipulation has been around forever, but it was harder for a scam artist to perpetrate scams employing manipulation of the victim in the era of slower payments processing. Early electronic payments fraud scams involved taking advantage of the slow pace of check processing (used by the fraudster to send money to the victim) compared to the quicker pace of electronic payments (used by the victim, at the instruction of the fraudster, to send payments to the fraudster). In one such scam, a perpetrator sends a phony check (sometimes certified) to the victim with instructions to wire money to the perpetrator. The victim, who may not understand a deposited check takes some time to clear and is slower than wire transfers, wires money out of their account to the perpetrator, only to find out later that the check is drawn on a non-existent account. The check is returned (bounces), and the victim is forced to cover the loss from the money paid out.[9]

This is exactly what happened in the case of *Valley Bank of Ronan v. Hughes*.[10] In that case, Mr. Hughes received from his swindlers four checks, two of them cashier's checks, totaling just over $1.6 million. On a Friday in 2002, he deposited the checks into his account at Valley Bank and received assurances from the teller that the cashier's checks, for $1.5 million, were the "same as cash." On the following Tuesday, he ordered his bank to wire $800,000 to his swindlers, who had an account in Amman, Jordan. This outbound payment via wire was completed before Mr. Hughes learned that the checks were no good. The $800,000 was gone, and Mr. Hughes had overdrawn his account by $800,000. Mr. Hughes had no choice but to use his retirement savings to pay part of the debt to Valley Bank, and he lost his home in foreclosure to pay the rest.

The "mystery shopper" scam similarly relies on the time disparity between payment methods and works like this:

---

9. NAT'L CONSUMER LAW CTR., CONSUMER BANKING AND PAYMENTS LAW § 4.8.6 (6th ed. 2018); *see also* Aresty Int'l Law Firm, P.C. v. Citibank, N.A., 677 F.3d 54 (1st Cir. 2012); Chino Com. Bank v. Peters, 118 Cal. Rptr. 3d 866 (Cal. Ct. App. 2010); Clark H.C. Lacy, *The Witch's Brew: Nigerian Schemes, Counterfeit Cashier's Checks, and Your Trust Account*, 61 S.C. L. REV. 753 (2010).

10. Valley Bank of Ronan v. Hughes, 147 P.3d 185 (Mont. 2006).

> The payee is 'hired' to observe customer service at her bank or a Western Union office. The payee is told she will receive a check for more than the amount the payee is to be paid for evaluating the bank or Western Union office. The payee is instructed to wire to the drawer the difference between the face value of the check and the payee's pay for conducting the observation. For example, a payee might be told that she will be paid $200 to observe a Western Union office. The payee will be sent a check for $500 and instructed to wire $300 back to the drawer from the Western Union office. It looks to the payee as though she will be making $200 from the 'employment.' When the $500 check bounces, the check will be returned to the Western Union office, which can enforce the check against the payee on the payee's indorser's obligation. The $300 sent to the scam artist is only recoverable if the payee can find the scam artist.[11]

Another check scam that takes advantage of a slow payment can happen when a buyer of goods or services pays the seller by check and the seller sends the goods or performs the services before the check has cleared.[12] The check ends up bouncing, and the seller has lost the goods.

Each of these scams relies on the competing processing times between payments systems. So long as the crook receives money through a payment system that moves faster than the system through which the victim was sent money, the crook will "win the race" and make off with the victim's money. While check processing has sped up, it is still slower than electronic forms of payment. Thus, these schemes that rely on slow inbound payments from the perpetrator to the victim and faster outbound payments from the victim to the perpetrator persist.

C. *Manipulation Fraud Schemes Involving P2P Payments*

As payment processing and settlement of all types has sped up, reducing the time differentials between incoming and outgoing payments even when different payment methods are used, fraudsters have adapted their craft, taking advantage of both the speed at which payments are processed and advances in technology. The problem has become particularly acute in the world of P2P payments, where fraudsters can take advantage of both the platform's speed and irrevocability.

---

11. CONSUMER BANKING AND PAYMENTS LAW, *supra* note 9, at 154.
12. *Id.*

P2P payments became extraordinarily popular during the COVID-19 pandemic, which began in 2020—a time when contactless payment became imperative.[13] These types of payments process and clear almost instantaneously and cannot be clawed back even moments after the transaction is initiated.[14] Once a scammer convinces their target to hit "send" on the payment or to inadvertently turn over information that can be used to access the account, the game is over. There is no time to reconsider, stop the payment, or realize that one has been duped into providing account access.

Some of the fraud scams reported on P2P payment platforms are quite simple. Fraudsters advertise an item for sale, insist on payment instantaneously before parting with the item sold, and never send the item.[15] Alternatively, they create phony identities on dating websites and convince unsuspecting new partners to send money for some urgent (and false) purpose.[16] Other scams are more sophisticated but still bear some of the hallmarks of earlier scams, relying on slow incoming payments processing and fast—now instantaneous—outgoing ones. This is the sort of scam perpetrated against a video editor who was promised $300 for editing a video.[17] His "client" "accidentally" sent him a check

---

13. GEOFFREY GERDES, CLAIRE GREENE, & XUEMEI (MAY) LIU, BD. OF GOVERNORS OF THE FED. RSRV. SYS., DEVELOPMENTS IN NON-CASH PAYMENTS FOR 2019 AND 2020: FINDINGS FROM THE FEDERAL RESERVE PAYMENTS STUDY (2021), https://www.federalreserve.gov/paymentsystems/december-2021-findings-from-the-federal-reserve-payments-study.htm [https://perma.cc/XQ76-3DSJ]; Letter from Sen. Robert Menendez, Sen. Elizabeth Warren, Sen. Jack Reed, Sen. Sherrod Brown, Sen. Chris Van Hollen, Sen. Sheldon Whitehouse, Sen. Bernard Sanders, and Sen. Tammy Duckworth to Richard Fairbank, Chairman and Chief Exec. Officer Cap. One Fin. Corp. (July 7, 2022), https://www.warren.senate.gov/oversight/letters/warren-menendez-reed-colleagues-demand-answers-from-big-banks-on-wide-spread-fraud-on-zelle-instant-payment-application [https://perma.cc/4LCA-DNFN]; Stacy Cowley, *Cash Faces a New Challenger in Zelle, a Mobile Banking Service*, N.Y. TIMES (June 12, 2017), https://www.nytimes.com/2017/06/12/business/dealbook/mobile-banking-zelle-venmo-apple-pay.html [https://perma.cc/CP68-QLV2].

14. Letter from U.S. Sens. to Robert Fairbank, *supra* note 13, at 1; Emily Mason, *Despite A Late Start, Bank-Owned Zelle Moves More Money Than Venmo and Cash App Combined*, FORBES (Sept. 8, 2022), https://www.forbes.com/sites/emilymason/2022/09/08/despite-a-late-start-bank-owned-zelle-moves-more-money-than-venmo-and-cash-app-combined/?sh=287bcd299d3f [https://perma.cc/6YZS-6XEV].

15. Cowley & Nguyen, *supra* note 7; Mason, *supra* note 14.

16. *What to Know About Romance Scams*, FED. TRADE COMM'N (Aug. 2022), https://consumer.ftc.gov/articles/what-know-about-romance-scams#whatis [https://perma.cc/7L27-8DXM] (In 2021, the Federal Trade Commission received reports of $547 million in losses to romance scams.). *See also* Emma Fletcher, *Romance Scammers' Favorite Lies Exposed*, FED. TRADE COMM'N: CONSUMER PROT. DATA SPOTLIGHT (Feb. 9, 2023), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed [https://perma.cc/Y7HH-9HMV].

17. Chris Flanagan, *"They're Not Robots Talking to You. They're Actual People." Zelle App Users Warn of Latest Scams*, BOS. 25 NEWS (Mar. 23, 2022, 8:23 AM), https://www.boston25news.com/news/massachusetts/theyre-not-robots-talking-you-theyre-actual-people-zelle-app-users-warn-latest-scams/WJZVXE23JZFCTPBD5XOPZZXF6I/ [https://perma.cc/7WT4-NC4P].

for $3,000 rather than $300 and asked the videographer to return the overpayment of $2,700 through Zelle. The videographer waited until he thought the check had cleared, then paid the money to his "client" through Zelle. The check bounced, and the account from which the videographer had received the video that was to be edited disappeared. The videographer could not recover the $2,700 out of which he had been scammed.[18]

Perhaps the most troubling type of scam occurring on P2P payments platforms involves the use of technology to deceive the target into making a payment to the scam artist. These scams often employ "spoofing," in which a scammer "deliberately falsifies the information transmitted to [the victim's] caller ID display to disguise their identity" in order to make it look like the call or text is coming from a business or individual known to the victim.[19] Victims of spoofing are deceived into believing they are paying a legitimate debt to a legitimate company[20] or paying a government agency, non-profit organization, university or charity—when in fact the payment is going to the fraudster.[21] In perhaps the most pernicious scam involving technology and spoofing, called a "me-to-me" scam, the scam artist sends a communication—usually a text—to the target that looks like it came from the target's bank. The scam artist, posing as an employee of the bank, claims to have detected a fraudulent payment out of the target's account. The scam artist then convinces the target that the fraudulent payment can be stopped if the target sends money to themself through Zelle in order to recover the phony fraudulent transfer.[22] In the meantime, the scam artist has

18. *Id.*

19. *Caller ID Spoofing*, FED. COMMC'NS COMM'N (Mar. 7, 2022), https://www.fcc.gov/spoofing [https://perma.cc/E2QD-PAFG]; OFF. OF SEN. ELIZABETH WARREN, FACILITATING FRAUD: HOW CONSUMERS DEFRAUDED ON ZELLE ARE LEFT HIGH AND DRY BY THE BANKS THAT CREATED IT 4 (2022) [hereinafter FACILITATING FRAUD], https://www.warren.senate.gov/imo/media/doc/ZELLE%20REPORT%20OCTOBER%202022.pdf [https://perma.cc/3W9R-5RSF]; Healey, *supra* note 8.

20. FACILITATING FRAUD, *supra* note 19, at 4.

21. FIN. CRIMES ENF'T NETWORK, FIN-220-A003, ADVISORY ON IMPOSTER SCAMS AND MONEY MULE SCHEMES RELATED TO CORONAVIRUS DISEASE 2019 (COVID-19) 2 (2020), https://www.fincen.gov/sites/default/files/advisory/2020-07-07/Advisory_%20Imposter_and_Money_Mule_COVID_19_508_FINAL.pdf [https://perma.cc/5ACQ-2C78].

22. Cowley & Nguyen, *supra* note 7; *see* Mason, *supra* note 14; Ashli Lincoln, *Customers Scammed on Zelle Banking App Have Virtually No Fraud Protection, Consumer Advocates Say*, WSB-TV ATLANTA (Mar. 22, 2022, 4:53 PM), https://www.wsbtv.com/news/local/customers-scammed-zelle-banking-app-have-virtually-no-fraud-protection-consumer-advocates-say/KKSK5LIOWVD47PF2UPTR4IMXSA/ [https://perma.cc/LPJ5-3ESR]; Gordon Severson, *Two Minnesota Women Were Tricked by the Same Scam on Zelle, Here's How You Can Protect Yourself*, KARE 11 (Mar. 22, 2022, 10:22 PM), https://www.kare11.com/article/money/minnesota-women-tricked-bythe-same-scam-on-zelle-heres-how-you-can-protect-yourself/89-3016a498-c8db-407a-ab1f-632f24204d9a [https://perma.cc/4UJA-SHRQ]; Carlos Granda, *Calif. Woman Loses Over $18K through 'Zelle' After Scammers Text, Call Her Pretending to be Bank*, 2 ABC 7 (Mar. 14, 2022), https://abc7news.com/zelle-scam-electronic-withdrawals-bank-of-america/11650620/ [https://perma.cc

already taken over the target's phone number, so the target's payment, purportedly to themselves, actually goes to the scam artist. A recent *New York Times* article described just this type of scam, in which a Wells Fargo me-to-me victim sent money to a scam artist after receiving a text message that appeared as if it came from Wells Fargo's fraud department. The victim lost $500 to the scam artist before realizing that the whole thing was a scam.[23] According to the Federal Trade Commission, this was the top type of text message scam reported by consumers to the FTC in 2022, and the average loss to a consumer who fell victim to this scam was $3000.[24]

At times, it can be unclear how a criminal accessed the victim's bank account. Money simply vanishes from the account, sent through Zelle to some unknown person, never to be seen again.[25] One survey suggested that P2P payment services were used to transfer money in 25% of cases involving accounts that were accessed without the account owner's consent.[26]

D. *Zelle*

Of all the P2P payments platforms currently available, the one that has received the most attention is Zelle. Zelle is owned by a company called Early Warning Services, LLC, a Delaware corporation jointly-owned by seven of the U.S.'s largest banks: JPMorgan Chase, Bank of America, Wells

---

/X42F-ESWF]; Ben Bradley & Andrew Schrodter, *As Scams Soar on Zelle, So Does Debate Over Who's to Blame*, WGN CHICAGO (Mar. 31, 2022), https://wgntv.com/news/wgn-investigates/as-scams-soar-on-zelle-so-does-debate-over-whos-to-blame/ [https://perma.cc/4AFS-3DKW]; John Matarese, *Zelle Scam Steals Over $10,000 from Woman*, WCPO CINCINNATI (Oct. 21, 2021), https://www.wcpo.com/money/consumer/dont-waste-your-money/zelle-scam-steals-over-10-000-from-woman [https://perma.cc/QZ5C-4DEV]; Cowley, *supra* note 13; FACILITATING FRAUD, *supra* note 19, at 4.

23. Cowley & Nguyen, *supra* note 7. Sometimes the scam will involve changing the phone number on a Zelle account by sending the victim a two-factor authentication code that allows the scammer to change the phone number on the account to the scammer's phone number. Healey, *supra* note 8.

24. Press Release, Fed. Trade Comm'n, New FTC Data Analysis Shows Bank Impersonation is Most-Reported Text Message Scam (June 8, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/06/new-ftc-data-analysis-shows-bank-impersonation-most-reported-text-message-scam [https://perma.cc/U9PP-8X9X]; *IYKYK: The Top Text Scams of 2022*, FED. TRADE COMM'N: CONSUMER PROT. DATA SPOTLIGHT (June 8, 2023), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/06/iykyk-top-text-scams-2022 [https://perma.cc/F9XN-LGNZ].

25. Stacy Cowley & Lananh Nguyen, *When Customers Say Their Money Was Stolen on Zelle, Banks Often Refuse to Pay*, N.Y. TIMES (June 21, 2022), https://www.nytimes.com/2022/06/20/business/zelle-money-stolen-banks.html [https://perma.cc/TXA4-QZK5].

26. *Id.*

Fargo, U.S. Bank, PNC Bank, Truist, and Capital One.[27] In 2017, Zelle's first year of operation, Zelle processed 247 million transactions, worth $75 billion.[28] By 2021, that figure had grown to 1.8 billion transactions worth $490 billion.[29] In October 2022, the company announced that in its first five years it had handled "more than 5 billion transactions involving $1.5 trillion."[30] Between 2021 and 2022 alone, Zelle saw a 49% increase in the number of payments it processed and a 59% increase in the amount of money it processed.[31] Although Zelle is not the only P2P payment platform, it is the largest, in part because it is integrated with the online banking and mobile apps offered by its large bank owners.[32] By 2022, in addition to serving customers at its owners' financial institutions, Zelle had also partnered with "nearly 1,700 banks and credit unions representing 619 million checking, savings[,] and money markets accounts, or about 79% of all such accounts in the United States."[33] That's a lot of bank customers with ready access to Zelle.

Fraud committed through Zelle has been the subject of much scrutiny and criticism from customers, the press, legislators, and regulators alike. Beginning in April 2022, U.S. senators Elizabeth Warren (D.-Mass), Robert Menendez (D-N.J.), and Jack Reed (D-R.I.), along with other members of United States Senate Committee on Banking, Housing, and Urban Affairs, tried to scope the fraud loss problem from financial institution customers who use Zelle.[34] The committee

27. *See* EARLY WARNING, https://www.earlywarning.com/about [https://perma.cc/WM6Z-DPTC] (provides information about Early Warning Services, LLC and its ownership) (last visited Jan. 20, 2024); *see also Early Warning Services, LLC*, CONSUMER FIN. PROT. BUREAU, https://www.consumerfinance.gov/consumer-tools/credit-reports-and-scores/consumer-reporting-companies/companies-list/early-warning-services/ [https://perma.cc/C23B-FYJS] (for further information regarding Early Warning Services, LLC and its ownership) (last visited Jan. 20, 2024). That the company is a Delaware company can be seen from its filings with the Arizona Corporations Commission, publicly available at the Corporation Commission's website. *See* ARIZONA CORPORATION COMMISSION, https://azcc.gov/ [https://perma.cc/JXZ2-DBSY] (last visited Feb. 18, 2024). Size rankings are from the Federal Reserve Statistical Release, Large Commercial Banks ranked by consolidated assets as of December 31, 2023. *See Insured U.S.-Chartered Commercial Banks That Have Consolidated Assets of $300 Million Or More, Ranked By Consolidated Assets*, FED. RESERVE STAT. RELEASE, https://www.federalreserve.gov/releases/lbr/current/ [https://perma.cc/BX8T-Q6F4] (last visited Feb. 18, 2024); *see also* FACILITATING FRAUD, *supra* note 19, at 3; Healey, *supra* note 8; Cowley, *supra* note 13.

28. Cowley, *supra* note 13; Healey, *supra* note 8.

29. Cowley & Nguyen, *supra* note 7; Cowley, *supra* note 13; Letter from U.S. Sens. to Robert Fairbank, *supra* note 13.

30. Healey, *supra* note 8.

31. Tom Groenfeldt, *Covid-19 Spurs Greater Use of Zelle and Venmo Payments*, FORBES (Feb. 8, 2022, 3:06 PM), https://www.forbes.com/sites/tomgroenfeldt/2022/02/08/covid-19-spurs-greater-use-of-zelle-and-venmo-payments/?sh=45ca2d301bba [https://perma.cc/9MBP-NRBW].

32. Mason, *supra* note 14 (other, older P2P platforms include PayPal, Venmo (owned by PayPal), and CashApp).

33. *Id*.

34. Letter from U.S. Sens. to Richard Fairbank, *supra* note 13, at 3.

requested that Early Warning Services and its financial institution owners provide data on fraud committed through Zelle.[35] Early Warning Services responded that the value of fraudulent transactions processed through Zelle was less than .09% of the total payments processed since 2017.[36] Although, if true, this is a small percentage of the payments processed by Zelle, it translates to a lot of money: $440 million in fraudulent transactions in 2021, given that $490 billion was paid through Zelle in 2021.[37] Early Warning Services has since said that "99.9% of the 1.8 billion in peer-to-peer payments sent last year were processed without a hitch."[38] Assuming this references $1.8 billion, and means that there was fraud present in only .01% of Zelle transactions (which may be an improper assumption, since payments induced by fraud can also be "processed without a hitch"), this would still mean that Zelle users lost $1.8 million in 2021. Moreover, the percentage of individual Zelle users impacted by fraud is likely higher than the percentage of Zelle transactions that are fraudulent, because many Zelle users will engage in multiple transactions, only one of which may be fraudulent.

After a Senate hearing on Zelle fraud in September 2022,[39] three of Zelle's seven owner institutions (PNC, U.S. Bank, and Truist) responded to the senators' April 2022 request for information from EWS, providing complete data sets to Senator Elizabeth Warren, who then issued a report on the data.[40] In that data, these three responding banks reported 35,848 cases of scams perpetrated through Zelle in 2021 and the first half of 2022, valued at just under $26 million in payments.[41] Bank of America,

---

35. Letter from Sen. Elizabeth Warren to Al Ko, Early Warning Services, LLC (Dec. 21, 2022), https://www.warren.senate.gov/imo/media/doc/2022.12.21%20Letter%20to%20EWS%20re%20Zelle%20Policy%20Changes.pdf; Letter from U.S. Sens. to Richard Fairbank, *supra* note 13, at 4; *see also Annual Oversight of the Nation's Largest Banks before Sen. Comm. on Banking, Housing, and Urban Affairs*, 107th Cong. 2, at 2:04:56-2:06:30 (2022) (statement of Sen. Elizabeth Warren), https://www.banking.senate.gov/hearings/annual-oversight-of-the-nations-largest-banks [https://perma.cc/2WDG-5WUP].

36. Letter from U.S. Sens. to Richard Fairbank, *supra* note 13, at 3.

37. Letter from U.S. Sens. to Richard Fairbank, *supra* note 13, at 1, 3. It is important to note that it is unclear whether this amount includes payments induced by scams, as opposed to just payments not authorized by the account holder. Letter from U.S. Sens. to Richard Fairbank, *supra* note 13, at 2–3.

38. Kate Berry, *How Much Fraud is on Zelle? Depends on Who You Ask*, AMERICAN BANKER (Oct. 17, 2022, 12:05 PM), https://www.americanbanker.com/news/how-much-fraud-is-on-zelle-depends-who-you-ask [https://perma.cc/76NS-SB5C]; Healey, *supra* note 8.

39. *Annual Oversight of the Nation's Largest Banks*, *supra* note 34. *See* Press Release, Elizabeth Warren, U.S. Senate, At Hearing, Warren Blasts Bank CEOs on Failure to Protect Consumers From Zelle Fraud (Sept. 22, 2022), https://www.warren.senate.gov/newsroom/press-releases/at-hearing-warren-blasts-bank-ceos-on-failure-to-protect-consumers-from-zelle-fraud [https://perma.cc/GRD7-8DLD], for a transcript of Senator Elizabeth Warren's exchange with witnesses over Zelle fraud.

40. FACILITATING FRAUD, *supra* note 19.

41. *Id.* at 6.

which appears to have only responded in part, reported 157,030 instances of scams perpetrated through Zelle in 2021 and the first eight months of 2022, valued at $187.9 million.[42] Wells Fargo provided evidence that its customers "are reporting fraud and scams on Zelle at a rate that is nearly 2.5 times higher this year than that of 2019."[43] It is no wonder that Zelle has been called "a favorite of fraudsters" and the "preferred tool for grifters."[44]

Victims of fraud are often unable to recover the money fraudulently paid to scammers through their financial institutions.[45] For example, the Zelle data supplied to Senator Warren from PNC, U.S. Bank, and Truist indicate that only 10% of fraud victims who paid through Zelle recovered their money through their financial institution and only $2.9 million (11.2% of the money paid to reported scammers) was recovered by the victims.[46] This may be in part because Early Warning Services and its owner banks interpret the Electronic Funds Transfer Act[47] and its Regulation E[48] to only require them to provide refunds to their customers when a Zelle payment is made by someone who accessed the customer's account without authority to do so, not when the customer is defrauded into making a Zelle payment themselves.[49] (Part III(A) of this Article will discuss Regulation E).

The Zelle data turned over to the Senate and reported in the media likely represents problems encountered by consumers on other P2P payments platforms, and thus likely underestimates the scale of the problem. Indeed, one survey of eight banks, conducted by the Bank Policy Institute, found that fraud rates were much higher on PayPal (three times higher) and Cash App (six times higher) than on Zelle.[50]

---

42. *Id.*

43. Letter from Sen. Elizabeth Warren to Charles Scharf, CEO and President, Wells Fargo & Co. (Oct. 6, 2022), https://www.warren.senate.gov/oversight/letters/warren-wells-fargos-fraud-and-scams-on-zelle-are-higher-than-other-banks-and-increasing-rapidly-renews-call-for-missing-data [https://perma.cc/C439-YU9H].

44. Cowley & Nguyen, *supra* note 7.

45. *See, e.g.*, *id.*; Cowley & Nguyen, *supra* note 25; Letter from U.S. Sens. to Richard Fairbank, *supra* note 13, at 2.

46. FACILITATING FRAUD, *supra* note 19, at 6.

47. Electronic Funds Transfer Act, 15 U.S.C. § 1693.

48. Electronic Fund Transfers Regulation E, 12 C.F.R. § 1005 (2011).

49. FACILITATING FRAUD, *supra* note 19, at 2–3, 5–7; Letter from U.S. Sens. to Richard Fairbank, *supra* note 13, at 2–3; Cowley & Nguyen, *supra* note 7; Berry, *supra* note 38.

50. Tara Payne, *The Data Shows that Zelle Is the Safest Way for Consumers to Move Their Money*, BANK POL'Y INST. (Sept. 19, 2022), https://bpi.com/the-data-shows-that-zelle-is-the-safest-way-for-consumers-to-move-their-money/ [https://perma.cc/XT9J-6W7F]. For a detailed report on fraud committed through Cash App, *see Block: How Inflated User Metrics and 'Frictionless" Fraud Facilitation Enabled Insiders to Cash Out Over $1 Billion*, HENDENBERG RSCH. (Mar. 23, 2023), https://hindenburgresearch.com/block/# [https://perma.cc/9KSK-MYMV].

A recent study by the Pew Research Center found that only 36% of U.S. adults use Zelle, but 57% use PayPal, 38% use Venmo, and 26% use Cash App.[51] The Pew study found that 76% of Americans used at least one of the identified payment platforms (Zelle, PayPal, Venmo, and Cash App).[52] Given this data, fraud likely affects many more consumers than we know. The Pew study supports this suspicion. It found that 13% of people who have used PayPal, Venmo, Zelle, or Cash App say they have sent someone money and later realized it was a scam, while a similar share (11%) report they have had their account hacked.[53]

III. SOLUTIONS

In a perfect world, it would be easy to detect and catch those individuals perpetrating and benefitting from payment scams and fraud. There are certainly plenty of criminal and civil statutes and causes of action that can be employed against these crooks. The problem is (and always has been) finding the crook—and being able to do so before the money is gone. It is for this reason that laws governing all payments have liability-assigning provisions in the likely event that the perpetrator cannot be found or is insolvent. When the bad guy cannot be found, the question becomes who, other than the bad guy, will bear the losses caused by fraud.

This is the essential question regarding the burgeoning P2P payment system. Are the losses from fraud going to be borne by the millions of Americans who are losing billions of dollars through fraud committed with the aid of instant, P2P payment platforms such as Zelle? Or should the payment system through which these payments are processed bear all or some of the loss through post-payment remedies? Should liability for these payments rest with the financial institutions that bank the crooks and money launderers and provide these fraudsters with access to the payment system?

There are many reasons why the financial institutions that own and operate P2P payment platforms should bear the losses from manipulation fraud on P2P payments systems rather than consumers. First, financial

---

51. Monica Anderson, *Payment Apps like Venmo and Cash App Bring Convenience – And Security Concerns – To Some Users*, PEW RSCH. CTR. (Sept. 8, 2022), https://www.pewresearch.org/short-reads/2022/09/08/payment-apps-like-venmo-and-cash-app-bring-convenience-and-security-concerns-to-some-users/ [https://perma.cc/2ZB3-PKN4] (looking at the age range, ethnicity, race, and household income of users of each of the four payment platforms).

52. *Id.*

53. *Id.*

institutions have many tools at their disposal to prevent and detect fraud.[54] Making financial institutions liable for fraud committed on P2P payment platforms will incentivize financial institutions to continually develop and improve fraud detection capabilities. This is exactly what has happened in the credit card space, where, because of statutes assigning liability to credit card issuers, financial institutions developed robust fraud monitoring capabilities and the ability to confirm authorized use in real time. (Anyone who has tried to use their own credit card for a purchase and gotten a fraud alert from their bank knows just how fast these tools are). Second, the types of losses suffered by consumer victims on P2P payment platforms can be devastating to a single consumer but manageable when shared across and absorbed by the banking system. So long as fraud losses are collectively low (as Zelle claims), the costs to the system as a whole will not be tremendous. If losses become high, the payment system is flawed, and the larger problem will need to be addressed.

The balance of this Article proposes statutory and regulatory changes that would place the loss for fraudulent P2P payments on the financial institutions that own and operate P2P payment platforms rather than on consumers. These changes to the law will protect victims of fraud and scams on P2P payment platforms, bring the rules governing loss from electronic payments fraud into the twenty-first century, and incentivize financial institutions to protect the U.S. financial system and consumers from fraudsters and scam artists who use P2P platforms to ply their trade.

A. *Solutions involving the Electronic Fund Transfer Act*

The first set of solutions involves the Electronic Fund Transfer Act (EFTA)[55] and its Regulation E.[56] At the outset, it is important to note two things about EFTA and Regulation E. First, EFTA's purpose is to provide

54. Financial institutions have many incentives to guard against fraud. First, financial institutions are liable for fraud or required to guard against fraud by many laws, including those discussed in this article and those required by other provisions, such as the Truth in Lending Act's Credit Card provisions. *See* 15 U.S.C. § 1643; 12 C.F.R. § 1026.12(b). Financial institutions also must guard against risks fraud imposes to profitability, reputation, and supervisory risk. It is for this reason that many vendors offer fraud detection systems to financial institutions. One example of these is offered by LexisNexis Risk Solutions. *See Expand Business Growth without Increasing Risk Exposure*, LEXISNEXIS RISK SOLUTIONS, https://risk.lexisnexis.com/financial-services [https://perma.cc/S9RA-4JE8] (last visited Sep. 29, 2023). Another is offered by SEON. *See* PJ Rohall, *Fraud Detection and Prevention in Banking Explained*, SEON (Aug. 11, 2023), https://seon.io/resources/banking-fraud-detection-and-prevention/ [https://perma.cc/BD8G-BDHY].

55. Electronic Fund Transfer Act, 15 U.S.C. § 1693.

56. Electronic Fund Transfers Regulation E, 12 C.F.R. § 1005 (2011).

for "individual consumer rights."[57] Second, instantaneous P2P payments are electronic fund transfers that clearly fall within EFTA's scope.[58] Whether EFTA (and its Regulation E) offers solace to victims of P2P fraud turns on whether such payments are deemed "authorized" or "unauthorized" under EFTA or, in the alternative, whether payments initiated by an authorized party who has been manipulated, defrauded, or conned into sending a payment are deemed as payments made in "error" under EFTA.

1. Classify payments by an authorized party who has been manipulated, defrauded, or conned into sending a payment as "unauthorized" payments under EFTA

Payments initiated by the consumer should be deemed unauthorized "if the consumer's authorization or initiation of the electronic fund transfer was fraudulently induced."[59]

One way to provide relief to those defrauded into sending payments through Zelle and other P2P payment platforms would be to classify these payments as "unauthorized" under EFTA.[60] Under EFTA, a consumer has no or limited liability for unauthorized payments made out of the consumer's account. The current statutory and regulatory scheme deems a payment made by someone who defrauds a victim out of their debit card or account access information as unauthorized. But many take the position that a payment made by someone who defrauds a victim into hitting "send" on the payment himself or herself is authorized—leaving the victim with no remedy under EFTA and Regulation E.

This Section discusses the electronic payments environment at the time EFTA was adopted and the statutory and regulatory history of EFTA. In particular, this Section discusses why and how unauthorized payments were identified and defined. Ultimately, this Section concludes that there is no longer justification for allowing a consumer to recover money stolen out of their account when the fraudster persuades the consumer to hand over the consumer's bank account and routing number information, while not allowing a consumer to recover the money stolen when a fraudster convinces the consumer to take out their smart phone and send a payment through Zelle. Rather, EFTA and Regulation E should be interpreted and/or amended to designate

57. 15 U.S.C. § 1693(b); 12 C.F.R. § 1005.1(b).
58. 15 U.S.C. § 1693a(7); 12 C.F.R. § 1005.3.
59. Protecting Consumers From Payment Scams Act, H.R. __, 117th Cong. (2022).
60. 15 U.S.C. § 1693a(12).

payments made due to manipulation fraud as unauthorized. This would treat fraud as fraud and go a long way in shifting the loss for such payments onto the payment system and away from individual consumers. A key question is who would have the authority to make this change.

One possibility is that the Consumer Financial Protection Bureau (CFPB) has the authority to interpret EFTA in this way, without further amendment by Congress. This is certainly the position taken by several U.S. Senators in a July 20, 2022 letter to CFPB Director Rohit Chopra, urging Director Chopra to draft rules that "keep pace with the growth of instant payment apps, like Zelle…to ensure that banks are on the hook to help consumers who've been scammed get their money back."[61] But it is possible that the fix would need to come from Congress itself, given the language and history of EFTA, both of which will be discussed next.

EFTA was adopted in the early days of electronic payments. The first consumer-usable form of electronic payment was the automated teller machine, or "ATM."[62] The ATM was first made available in England in 1967 and arrived in the U.S. within two years.[63] Consumers were slow to warm to these mechanical teller-substitutes, which at the time were rumored to be "eating" cards and, since they were largely placed outside, prone to weather related troubles.[64] But by the 1980s, "ATMs were big business and most banks had adopted them."[65]

In the years between the introduction of the first ATM in 1969 and its more ubiquitous adoption by banks and consumers in the 1980s, lawmakers grappled with whether and how to regulate the emerging electronic payment system. In 1974, Congress took the first step by creating the National Commission on Electronic Fund Transfers.[66] The Commission was directed to conduct "a thorough study and

---

61. Press Release, Sen. Jack Reed, U.S. Senators to CFPB: Hold Banks That Own Zelle Accountable for Inadequate Protections to Stop Fraudulently Induced Payments to Crooks (July 20, 2022), https://www.reed.senate.gov/news/releases/us-senators-to-cfpb-hold-banks-that-own-zelle-accountable-for-inadequate-protections-to-stop-fraudulently-induced-payments-to-crooks [https://perma.cc/5L7R-BVPQ].

62. *See* Kevin Wack & Alan Kline, *The Evolution of the ATM*, AM. BANKER (May 23, 2017, 2:05 PM), https://www.americanbanker.com/slideshow/the-evolution-of-the-atm [https://perma.cc/TVE9-VUUN]; Bernardo Bátiz-Lazo, *A Brief History of the ATM: How Automation Changed Retail Banking, an Object Lesson*, THE ATLANTIC (Mar. 26, 2015), https://www.theatlantic.com/technology/archive/2015/03/a-brief-history-of-the-atm/388547/ [https://perma.cc/5XWV-JHWC].

63. *See* Wack & Kline, *supra* note 62; Bátiz-Lazo, *supra* note 62.

64. *See* Bátiz-Lazo, *supra* note 62; Linda Rodriguez McRobbie, *The ATM is Dead. Long Live the ATM!*, SMITHSONIAN MAG. (Jan. 8, 2015), https://www.smithsonianmag.com/history/atm-dead-long-live-atm-180953838/ [https://perma.cc/59N4-NDHN].

65. McRobbie, *supra* note 64; *see also* Bátiz-Lazo, *supra* note 62; Ronald L. Winkler, *The National Commission on Electronic Fund Transfers: Problems and Prospects*, 1977 WASH. U. L. Q. 507, 507 (1977).

66. *See* 12 U.S.C. § 2401.

investigation and recommend appropriate administrative action and legislation necessary in connection with the possible development of public or private electronic fund transfer systems…."[67] In conducting its work, the Commission was tasked with taking into account the effect that the developing electronic payment system would have on financial institutions and on consumers. Specifically, the Commission was ordered to look at "the need to afford maximum user and consumer convenience; the need to afford maximum user and consumer rights to privacy and confidentiality; and the need to protect the legal rights of users and consumers."[68] In the end, the Commission was to develop "recommendations to Congress and the President regarding appropriate administrative action and legislation necessary in connection with the possible development of public or private electronic fund transfer systems."[69]

After some delays related to the confirmation of its Chair, the Commission began its work in February 1976 and issued its final report on October 28, 1977.[70] The report addressed all aspects of the burgeoning EFT payment system, but it focused "particularly on the rights and responsibilities of consumers in EFT."[71] In its work and reports, the Commission focused on how to protect consumers from the most common risks of theft apparent at the time—the use by a thief of a stolen or found ATM card and PIN (personal identification number) to withdraw cash, make purchases, or authorize payments to a customer's approved list of payees—and the related question of whether a consumer would be deemed negligent for writing his "PIN" down near his ATM card.[72]

---

67. *Id.* § 2403.

68. *Id.* § 2403.

69. Request for Comment, 42 Fed. Reg. 21529, (April 27, 1977).

70. NAT'L COMM'N ON ELEC. FUND TRANSFERS, EFT IN THE UNITED STATES: POLICY RECOMMENDATIONS AND THE PUBLIC INTEREST (October 28, 1977); Winkler, *supra* note 65, at 511.

71. Request for Comment, *supra* note 69, at iii. The Commission's work was open to the public, as can be seen by many announcements of meetings and hearings in the Federal Register. *See*, e.g., Meeting Notice, 41 Fed. Reg. 12356 (March 25, 1976); Meeting Notice, 42 Fed. Reg. 8236 (Feb. 9, 1977); Meeting Amendment, 42 Fed. Reg. 13165 (March 9, 1977); Request for Comment, 42 Fed. Reg. 21529 (April 27, 1977); Meeting Notice, 42 Fed. Reg. 38684 (July 29, 1977).

72. NAT'L. COMM'N. ON ELEC. FUND TRANSFERS, EFT AND THE PUBLIC INTEREST: A REPORT OF THE NATIONAL COMMISSION ON ELECTRONIC FUND TRANSFERS 18 (February 1977); NAT'L COMM'N ON ELEC. FUND TRANSFERS, *supra* note 70, at 56. Although the question was not resolved, the Commission did briefly consider the impairment to consumer's rights by a payment system with no lag time between the purchase of goods or services and the time the payment for that good or service cleared. The Commission recognized that in an electronic environment where payments process immediately, the consumer loses his ability to engage in post transaction self-help through the right to stop payment (for checks) and the right to a refund on the purchase of certain goods and services when a credit card is used. If the transaction goes awry. NAT'L COMM'N ON ELEC. FUND TRANSFERS, *supra* note 70, at 49–50.

Soon after the Commission issued its interim and final reports, in February and October 1977 respectively, Congress began to hold hearings and draft bills related to electronic fund transfers, ultimately adopting EFTA in October 1978.[73] Much of the debate over the bill focused on how much liability consumers should have for unauthorized transfers from their account. Financial institutions argued that consumers should be liable for losses caused by their negligence, such as when a consumer wrote their PIN number on their debit card, kept the card and PIN near each other, gave the card to another person to use, or failed to report loss or theft of the card.[74] Consumer groups advocated for a flat $50 limitation on a consumer's liability for unauthorized use, regardless of the consumer's negligence—a legislative approach similar to that take for credit cards in the Truth in Lending Act.[75]

EFTA, as adopted in late 1978,[76] forged a compromise between these two liability approaches.[77] The statute provided then, and still states today, that if a transfer of funds is unauthorized, the consumer has no liability for the unauthorized transfer unless the transfer was made using an accepted card or means of access for which the financial institution provided a way to identify the person authorized to use the card.[78] Even if the unauthorized transaction involves an accepted card or means of access, the consumer's maximum liability is $50 when the consumer promptly reports the loss or up to $500 when the consumer does not

73. Electronic Fund Transfer Act, Pub. L. 95-630, § 907, 92 Stat. 3733 (HR 14297) (adding EFTA to the Consumer Credit Protection Act of 1968); Consumer Credit Protection Act, Pub. L. 90-321, 82 Stat. 146 (1968). For a legislative history of the Electronic Funds Transfer Act, see Roland E. Brandel & Eustace A. Olliff III, *The Electronic Fund Transfer Act: A Primer*, 40 OHIO ST. L. J. 531, 538–40 (1979).

74. Lewis M. Taffer, *The Making of the Electronic Fund Transfer Act: A Look at Consumer Liability and Error Resolution*, 13 UNIV. S.F. L. REV. 231, 237–38 (1979).

75. *Id.* at 238; 15 U.S.C. § 1643(a)(1)(A).

76. Consumer Credit Protection Act, Pub. L. 95-630, 92 Stat. 3728 (1978).

77. *See* Taffer, *supra* note 74, at 239.

78. 15 U.S.C. § 1693g(a) (2018). The statute defines the term "accepted card or other means of access" as a "card, code, or other means of access to a consumer's account for the purpose of initiating electronic fund transfers when the person to whom such card or other means of access was issued has requested and received or has signed or has used, or authorized another to use, such card or other means of access for the purpose of transferring money between accounts or obtaining money, property, labor, or services. 15 U.S.C. § 1693a(1) (2018). Regulation E defines "[a]ccess device" as "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." 12 C.F.R. § 1005.2. Regulation E says an access device "becomes an "accepted access device" when the consumer: (i) Requests and receives, or signs, or uses (or authorizes another to use) the access device to transfer money between accounts or to obtain money, property, or services; (ii) Requests validation of an access device issued on an unsolicited basis; or (iii) Receives an access device in renewal of, or in substitution for, an accepted access device from either the financial institution that initially issued the device or a successor." 12 C.F.R. § 1005.2.

report the loss or theft of the access device within two days.[79] This means that when the rules of EFTA and regulation are observed, losses from all unauthorized transactions are fully or largely born by the financial institution rather than the bank customer. In the statute, Congress defined an "unauthorized electronic fund transfer" as follows:

> the term 'unauthorized electronic fund transfer' means an electronic fund transfer from a consumer's account *initiated by a person other than the consumer* without actual authority to initiate such transfer and from which the consumer receives no benefit, but the term does not include any electronic fund transfer *(A) initiated by a person other than the consumer* who was furnished with the card, code, or other means of access to such consumer's account by such consumer, unless the consumer has notified the financial institution involved that transfers by such other person are no longer authorized, (B) initiated with fraudulent intent by the consumer or any person acting in concert with the consumer, or (C) which constitutes an error committed by a financial institution.[80]

In 1979 the Federal Reserve Board issued its first regulations under EFTA, called "Regulation E," which further defined a "unauthorized electronic fund transfer" as follows:

> (k) "Unauthorized electronic fund transfer" means an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit.

---

79. 15 U.S.C. § 1693g (2018). The statute also provides that the consumer is liable for losses that the consumer does not report within 60 days of the transfer appearing on the consumer's bank statement, but the bank has to establish that the losses "would not have occurred but for the failure of the consumer to report" the loss. 15 U.S.C. § 1693g(a)(2) (2018).

80. 15 U.S.C. § 1693a(12) (2018) (emphasis added). The text of this definition has not changed since adoption of EFTA in 1978, although the numbering was mistakenly changed in 2011 from subsection 11 to subsection 12 by the Dodd-Frank Wall Street Reform and Consumer Protection Act. In that act Congress replaced the word "Board" (as in the Federal Reserve Board) in subsection 3 to the word "Bureau". This would have been sufficient to change the Federal Reserve Board's authority to the newly created Consumer Financial Protection Bureau, but the statute also re-designates paragraphs (3) through (11) as paragraphs (4) through (12), so that now there is no subsection (3). Dodd-Frank Wall Street Reform and Consumer Protection Act. Pub. L. 111-203, § 1084(1)–(2), 124 Stat. 2081 (2010).

> The term does not include any electronic fund transfer (1) initiated by a person who was furnished with the access device to the consumer's account by the consumer, unless the consumer has notified the financial institution involved that transfers by that person are no longer authorized, (2) initiated with fraudulent intent by the consumer or any person acting in concert with the consumer, or (3) that constitutes an error committed by the financial institution. that is initiated by the financial institution.[81]

Based on these definitions, a key characteristic of an unauthorized payment (other than those that are made fraudulently by the consumer or in error) is that it must be initiated by a person *other* than the consumer.

In 1981, the Federal Reserve Board issued its first official staff interpretation of Regulation E, phrased in the form of questions and answers about EFTA, Regulation E, and electronic payments.[82] Less than two years later, the Board addressed, for the first time, the question of whether a payment is unauthorized if the consumer is "conned or forced to furnish another person with an access device for use in an ATM."[83] The Fed's answer? Yes, this is an unauthorized payment: "In the case of a con or a robbery, the consumer did not intend to authorize the use of the access device to make electronic fund transfers and, as a result, the transfers are unauthorized."[84] A few months later, the Fed changed the commentary to specifically state that if a consumer is "induced by fraud to furnish another person with an access device," transfers initiated at an ATM by the fraudster are unauthorized.[85] Two years later, the Fed went a step further and declared that transfers initiated by the consumer himself are unauthorized if the consumer is "forced by a robber (at gunpoint, for example) to withdraw cash at an ATM."[86]

---

81. Electronic Fund Transfers, 44 Fed. Reg. 18480, 18481 (March 28, 1979). EFTA gave the Federal Reserve Board the authority to issue regulations. Consumer Credit Protection Act Pub. L. 95-630, § 904, 92 Stat. 3730 (1978).

82. *See* Electronic Fund Transfers, 46 Fed. Reg. 46876 (Sept. 23, 1981).

83. Technical Amendments and Official Staff Commentary Update, 48 Fed. Reg. 4667, 4668 (Feb. 2, 1983).

84. *Id.*

85. Technical Amendments and Update to Official Staff Commentary, 48 Fed. Reg. 14880, 14881 (April 6, 1983).

86. Official Staff Commentary Update, 50 Fed. Reg. 13180, 13181 (April 3, 1985) ("Q 2-28: *Unauthorized transfers – forced initiation.* A consumer is forced by a robber (at gunpoint, for example) to withdraw cash at an ATM. Do the liability limits for unauthorized transfers apply? A. *Yes*. The transfer is unauthorized for purposes of Regulation E. Under these circumstances, the actions of the robber are tantamount to use of a stolen access device.").

In 1996, the Federal Reserve Board replaced the question-and-answer format of its official staff commentary with a more traditional structure, articulating its comments in numbered paragraphs of declaratory statements rather than questions and answers.[87] The content stayed pretty much the same, except the staff commentary expanded the robbery/fraud comment to cover all access devices to an account and all electronic withdrawals, not just those at an ATM. The new comment 2(m), on Unauthorized Electronic Fund Transfers, provided the following:

> 3. *Access device obtained through robbery or fraud.* An unauthorized EFT includes a transfer initiated by a person who obtained the access device from the consumer through fraud or robbery.
> 4. *Forced initiation*. An EFT at an automated teller machine (ATM) is an unauthorized transfer if the consumer has been induced by force to initiate the transfer.[88]

EFTA and Regulation E's focus on transactions initiated by a person other than the consumer who had the consumer's ATM card, and on how that person obtained the ATM card, made sense in an era when bank customers' only "electronic" access to their account involved a debit card that could be used at an ATM or point of sale. If you gave your kid your debit card, and your kid used the card, the transaction was authorized. If you decided you no longer wanted your kid to be able to use your debit card, you called your bank, and transactions thereafter were unauthorized. If your debit card was stolen, or you were defrauded into giving it to someone, and you let your bank know, you were fine. If your debit card was stolen, or you were defrauded into giving it to someone, and you failed to contact your bank, you were on the hook [for at least $500][89] for any transfers made or cash withdrawals using the debit card. It was a statutory scheme designed for an age where you needed a physical card to get into someone's account. If your card ended up in the hands of a thief or a con artist, there would be at least some time between the theft of your physical debit card and the thief's trip to a bank or point of sale. The whole regime—based on physical cards, delayed access to payments, and slow payment processing times—made sense in context. But, as one payments consultant recently observed, "Regulation E was never intended for instant money movement products."[90]

---

87. Official Staff Interpretations, 61 Fed. Reg. 19686, 19687 (May 2, 1996).
88. *Id.*
89. *See* Brandel & Olliff, *supra* note 73, at 556, and the footnote's accompanying text.
90. Cowley & Nguyen, *supra* note 25.

Given the 1980s banking context, legislators and regulators could not have anticipated that the greatest frauds perpetrated on consumers would not involve consumers being conned out of their debit card, but rather being conned into making a payment to a fraudster. Indeed, it would have been difficult to imagine that consumers would be able to deposit checks electronically and access their bank account online, let alone use a phone to transfer money instantaneously. It certainly was never in contemplation that a fraudster would be able to capture someone's telephone number and, through a series of fraudulent texts, steal money from a consumer's account. And yet, despite these massive changes in electronic payments over the last decade or so and the frauds committed against consumers through electronic payment systems, EFTA's and Regulation E's unauthorized use provisions have remained static.[91] The definition of "unauthorized transaction" in EFTA is the same today as it was in 1978. The unauthorized transfer rules in Regulation E, promulgated at first by the Federal Reserve Board, and since 2011 by the Consumer Financial Protection Bureau, have changed in form but not in substance.[92] The commentary designating as unauthorized any payment

---

91. Over the years, there have been some changes to EFTA and Regulation E. *See, e.g.*, Credit CARD Act of 2009, Pub. L. 111-24, §401(2), 123 Stat. 1734, 1751 (2009); 12 C.F.R. §1005.2 (2020). However, since adoption of the statute in 1978, and adoption of the Federal Reserve Board's first version of Regulation E, the definitions of an "unauthorized transaction," and provisions on limited liability have remained essentially the same.

92. The current regulation text, codified at 12 C.F.R. 1005.2(m), with changes since 1979 indicated, is as follows:

> ~~(k)~~(l) (m) "Unauthorized electronic fund transfer" means an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit.
>
> The term does not include any electronic fund transfer initiated:
>
> (1) ~~initiated by~~ By a person who was furnished ~~with~~ the access device to the consumer's account by the consumer, unless the consumer has notified the financial institution ~~involved~~ that transfers by that person are no longer authorized,
> (2) ~~initiated with~~ With fraudulent intent by the consumer or any person acting in concert with the consumer, or
> (3) ~~that constitutes an error committed by the financial institution. that is initiated by~~ By the financial institution or its employee.

The original final rule was adopted on March 28, 1979. 44 Fed. Reg. 18480, 18481 (March 28, 1979). An amendment later that year renumbered the subsection to be subsection (l) rather than (k) and changed the wording of subsection (l) three by striking the words "that constitutes an error committed by the financial institution" and substituting them with the words "that is initiated by the financial institution or its employee." 44 Fed. Reg. 59464, 59470 (Oct. 15, 1979). In 1996, when the Federal Reserve Board re-worked the regulation, they made only slight changes to the definition of an unauthorized transaction: moving the word "initiated" from the beginning of subsection

made using a device that was obtained through fraud has not changed since 1996.[93]

The only "new" development at the federal level was a compliance aid in the form of frequently asked questions that was issued by the CFPB in 2021.[94] But there was really nothing new in this guidance. As described by one well-known financial institution law firm, "While the FAQs help provide some clarity for financial institutions, they do not provide any new obligations or requirements under Regulation E."[95] The CFPB merely expounded on the long-standing commentary providing that an EFT initiated by someone who defrauds someone into sharing account access information is unauthorized. Specifically, the CFPB reiterated that "an EFT initiated by a fraudster using stolen credentials" is unauthorized, and provided the following examples of unauthorized EFTs of which it said it is "aware":

- A consumer shares their account access information in order to enter into a transaction with a third party, such as a merchant, lender, or employer offering direct deposit, and a fraudster obtains the consumer's account access information by hacking into the computer system of the third party. The fraudster then uses a bank-provided P2P payment application to initiate a credit push payment out of the consumer's deposit account.
- A consumer shares their debit card information with a P2P payment provider in order to use a mobile wallet. A fraudster then hacks into the consumer's phone and uses the mobile wallet to initiate a debit card transfer out of the consumer's deposit or prepaid account.

(l)(1) and (l)(2) to the end of the sentence before these subsections, and changing the initial letter in subsections 1-3 to have a capital letter. 61 Fed. Reg. 19662, 19669 (May 2, 1996). When the CFPB inherited Regulation E, it changed the designation of this subsection from (l) to (m) but made no other changes. Regulation E, 76 Fed. Reg. 81020, 81023 (Dec. 27, 2011). None these changes were substantive and there have been no further changes.

93. *See supra* notes 85, 86, and accompanying text. *Compare* Official Staff Interpretations, 61 Fed. Reg. 19686, 19687 (May 2, 1996), *with Official Interpretation of 2(m) Unauthorized Electronic Fund Transfer*, CONSUMER FIN. PROT. BUREAU, https://www.consumerfinance.gov/rules-policy/regulations/1005/2/#b-3-ii-C [https://perma.cc/9797-V4U5].

94. The "FAQ's" were issued on June 4, 2021. Garrett Fischer & Sarah Wade, *CFPB Provides Additional Guidance on Unauthorized Electronic Fund Transfers*, THOMPSON COBURN LLP (Nov. 4, 2021), https://www.thompsoncoburn.com/insights/blogs/bank-check/post/2021-11-04/cfpb-provides-additional-guidance-on-unauthorized-electronic-fund-transfers [https://perma.cc/SRZ3-YF6V]. The FAQ's were then updated again on December 13, 2021.

95. Jennifer E. Aguilar, *CFPB Updates Electronic Fund Transfers FAQs*, BALLARD SPAHR LLP (Jan. 3, 2022), https://www.consumerfinancemonitor.com/2022/01/03/cfpb-updates-electronic-fund-transfers-faqs/ [https://perma.cc/8D8B-JBBB].

- A thief steals a consumer's physical wallet and initiates a payment using the consumer's stolen debit card.[96]

The CFPB also reiterated that a transaction is unauthorized if "a third party fraudulently induces a consumer into sharing account access information that is used to initiate an EFT from the consumer's account," and provided the following examples:

> For example, the Bureau is aware of the following situations where a third party has fraudulently obtained a consumer's account access information, and thus, are considered unauthorized EFTs under Regulation E: (1) a third-party calling the consumer and pretending to be a representative from the consumer's financial institution and then tricking the consumer into providing their account login information, texted account confirmation code, debit card number, or other information that could be used to initiate an EFT out of the consumer's account, and (2) a third party using phishing or other methods to gain access to a consumer's computer and observe the consumer entering account login information.[97]

Finally, the Bureau reiterated that "a consumer who is fraudulently induced into providing account information has not furnished an access device under Regulation E."[98] (When a consumer gives or "furnishes" an access device to someone else and that device is used to transfer funds, the transaction is not unauthorized "unless the consumer has notified the financial institution involved that transfers by such other person are no longer authorized.")[99]

The CFPB FAQs recognize new methodologies for fraudulently obtaining an access device, but the basic rule stays the same. Thus, the current status is a statutory and regulatory regime that calls "unauthorized" a payment made by someone who defrauds a victim out of their debit card or account access information, while treating as authorized a payment made by someone who defrauds a victim into initiating the payment himself or herself. It is an antiquated system conceived of in the quaint debit card days of the early 1980s, and deeply inadequate for addressing the scams flourishing in the world of P2P payments.

---

96. *Electronic Fund Transfers FAQs, Error Resolution: Unauthorized EFTs*, CONSUMER FIN. PROT. BUREAU 2 (Dec. 13, 2021), https://files.consumerfinance.gov/f/documents/cfbp_electronic-fund-transfers-faqs.pdf [https://perma.cc/9YAF-MYPR] (see Question 4).

97. *Id.* at 12.

98. *Id.* at 12–13.

99. 15 U.S.C. § 1693a(12).

One way to address the dominant types of fraud present in the P2P electronic payment system would be to update the definition of "unauthorized" to eliminate the distinction between fraud that induces someone to hand their access device over to a fraudster and fraud that induces someone to hit "send" on a payment to a fraudster. Such a change to EFTA and Regulation E would be consistent with the purpose of EFTA, which is to protect consumers in the electronic payments environment,[100] and would bring EFTA's protections into modern times. The focus on who "initiates" the transaction is no longer relevant, given the advances in technology in the thirty years since the Federal Reserve announced that distinction in its 1981 commentary.[101] The key question, though, is who has the authority to bring EFTA into the modern world—is it the CFPB or Congress?

It is clear from the letter they sent to the CFPB that Senators Reed, Menendez, Warren, Brown, Cortez Masto, and Warnock believe that the CFPB can take this action without further Congressional enactments.[102] These Senators implored the CFPB to protect consumers when they are "tricked into opening an application *to transfer funds directly* to the fraudster" not just when they are "tricked into handing *over account information* to a fraudster who then initiates a transfer."[103] "Determining liability based on whether a consumer or a fraudster physically initiates a transaction," they said, "is antiquated" and "not suited for the current system, where consumers need only a cell phone number or username to send peer to peer payments from a mobile device with nearly instantaneous credits and debits."[104] They concluded that, "[o]ur nation's consumer protection rules must evolve to keep pace with the growth of instant payment services like Zelle." [105] And they urged the CFPB to, among other things, "issue guidance that a fraudulently induced transaction is an "unauthorized electronic fund transfer" under EFTA."[106] Senator Elizabeth Warren made a similar plea in a report on Zelle fraud issued by her office in October 2022, calling on the CFPB to "move quickly to strengthen and improve rules that prevent consumers from being safe

100. 15 U.S.C. § 1693(b); 12 C.F.R. § 1005.1(b) (2022).

101. *See Electronic Fund Transfers*, *supra* note 82.

102. Letter from Sen. Jack Reed, Sen. Robert Menendez, Sen. Elizabeth Warren, Sen. Sherrod Brown, Sen. Catherine Cortez Masto, & Sen. Warnock to Rohit Chopra, Director, Consumer Fin. Prot. Bureau (July 20, 2022), https://www.reed.senate.gov/news/releases/us-senators-to-cfpb-hold-banks-that-own-zelle-accountable-for-inadequate-protections-to-stop-fraudulently-induced-payments-to-crooks [https://perma.cc/BYQ6-57DN].

103. *Id.*

104. *Id.*

105. *Id.*

106. *Id.*

on Zelle, and ensure that banks reimburse them when they are defrauded or their money is stolen."[107]

This focus by several Senators on fraud committed through Zelle and other P2P platforms, and calls for action by the CFPB, has caused a bit of a panic in the financial services industry. Industry members have started to speculate that the CFPB will issue new guidance expanding Regulation E's coverage to situations in which "a customer is tricked into sending money to a scammer pretending to be a representative of his or her bank" and to classify as unauthorized "even those [transactions] approved by the consumer."[108] In opposition to this path, the financial services industry has argued that the CFPB does not have this authority to do this under EFTA, that shifting liability to financial institutions will force them to stop offering P2P services or charge for them, that consumers will be forced to wait for money paid to them, and that such a change would encourage consumers to commit fraud against their financial institutions.[109] At this juncture, it is unclear if the CFPB plans to go down this road.[110]

While it may be true that the EFTA scheme is "antiquated" and "not suited for the current system,"[111] the statutory language, defining an unauthorized electronic fund transfer as one "*initiated by a person other than the consumer*"[112] makes it unclear whether the CFPB has authority to expand the definition to include fraudulently induced payments. One could argue that the CFPB would be well within its EFTA regulatory authority by taking a broad view of the word "initiated".[113] The Oxford English Dictionary definition of "initiated" is "[t]o begin, commence, enter upon; to introduce, set going, give rise to, originate, 'start' (a course of action, practice, etc.)."[114] The online dictionary.com has a

107. FACILITATING FRAUD, *supra* note 19, at 2.

108. *See, e.g.*, Andrew Ackerman, *CFPB to Push Banks to Cover More Payment Services Scams*, WALL ST. J. (July 19, 2022), https://www.wsj.com/articles/consumer-bureau-to-push-banks-to-refund-more-victims-of-scams-on-zelle-other-services-11658235601 [https://perma.cc/F8TM-9A2E].

109. Letter from Nessa Feddis, Am. Bankers Ass'n, to Rohit Chopra, Director, Consumer Fin. Prot. Bureau (Oct. 27, 2022) (on file with author), https://www.aba.com/advocacy/policy-analysis/letter-to-cfpb-on-p2p-payments-and-scams [https://perma.cc/76QQ-VLAP]; *see also* Letter from U.S. Sens. to Rohit Chopra, *supra* note 102.

110. In March, it was reported that in regard to the question of "who is responsible for a fraudulently induced transfer if the customer physically hit the buttons" the CFPB has said, "The C.F.P.B. is aware of the problem and considering how best to address it." Cowley & Nguyen, *supra* note 7.

111. Letter from U.S. Sens. to Rohit Chopra, *supra* note 102.

112. 15 U.S.C. § 1693a(12), *supra* note 80 (emphasis added).

113. *Id.*

114. *Initiate*, OXFORD ENGLISH DICTIONARY, https://www.oed.com/view/Entry/96066?rskey=VGsJ9G&result=1#eid [https://perma.cc/MT5M-UD9D] (last visited Jan. 20, 2024).

similar definition: "To begin, set going, or originate."[115] It could certainly be argued that when a fraudster takes the first steps towards scamming the consumer, *this* is the initiation of the electronic transfer. Given this interpretation of the word "initiated," the CFPB would be well within the scope of its regulatory powers. On the other hand, there will be those who argue that, in cases where a consumer is scammed into "hitting the buttons," it is the consumer who has "initiated" the transaction.[116]

Given the two possible interpretations of EFTA's "*initiated by a person other than the consumer*"[117] language, it would behoove Congress to take action to address the problem. It appears that at least some members of the 117th Congress were cognizant of the need for Congress to address the definition of "unauthorized" in EFTA. During the 117th Congress, 2nd session, a draft bill was circulating in Congress, the "Protecting Consumers From Payment Scams Act," that would have amended the definition of an "unauthorized payment" as follows:

> (12) The term 'unauthorized or fraudulently induced electronic fund transfer'
> (A) means an electronic fund transfer from a consumer's account initiated by –
> (i) a person other than the consumer without actual authority to initiate such transfer; or
> (ii) the consumer, if the consumer's authorization or initiation of the electronic fund transfer was fraudulently induced; and
> (B) does not include any electronic fund transfer –
> (i) initiated by a natural person other than the consumer who was furnished with the card, code, or other means of access to such consumer's account by such consumer, unless –
> (I) the consumer has notified the financial institution involved that transfers by such other person are no longer authorized; or
> (II) the consumer was fraudulently or coercively induced to furnish the card, code, or other means of access;
> (ii) initiated by a consumer who has fraudulent intent, or anyone acting in concert with such a consumer; or

115. *Initiate,* DICTIONARY.COM, https://www.dictionary.com/browse/initiate [https://perma.cc/977L-KRJV] (last visited Jan. 20, 2024).

116. A recent (2023) addressed this issue directly, finding that the definition of unauthorized in EFTA did not cover manipulation fraud. Tristan v. Bank of Am., 2023 WL 4417271 (D. Ct. Ca. June 28, 2023).

117. 15 U.S.C. § 1693a(12), *supra* note 80 and accompanying text (emphasis added).

(iii) which constitutes an error committed by a financial institution."[118]

On April 28, 2022, the United States House of Representatives Committee on Financial Services held a hearing related in part to the bill entitled, "What's in Your Digital Wallet? A Review of Recent Trends in Mobile Banking and Payments."[119] But as of the writing of this Article, the bill has not been introduced. The discussion draft was pulled from the House Financial Services Committee's primary website after the seating of the 118th Congress, in which the majority changed from Democrats to Republicans. It was then made available on the website of the committee Democrats and is now part of the House records.[120]

2. Designate payments initiated by an authorized party who has been manipulated, defrauded, or conned into sending a payment as payments made in "error" under EFTA

"The agency should act to clarify and strengthen Regulation E and include fraud in the Regulation's error resolution purview, increasing the responsibility of banks to keep Zelle safe and to ensure that consumers will be protected."[121]

The second possible solution that would provide relief to those defrauded into sending payments through Zelle and other P2P payment platforms would be to designate payments initiated by an authorized party who has been manipulated, defrauded, or conned into sending a payment as payments made in "error" under EFTA.

When a payment is made in "error," the person from whose account the payment was made accrues specific legal rights.[122] When a consumer reports an "error," the institution is required to investigate the error promptly;[123] determine within ten business days if an error has occurred (which time can be extended up to forty-five days in certain

118. Protecting Consumers From Payment Scams Act, H.R. __, 117th Cong. (2022), https://www.congress.gov/117/meeting/house/115250/documents/BILLS-117pih-ProtectingConsumersFromPaymentScamsAct.pdf [https://perma.cc/YSV2-Z5BE].

119. Information about the hearing is available at *What's in Your Digital Wallet? A Review of Recent Trends in Mobile Banking and Payments*: *Hybrid Hearing on H.R. Before Task Force on Fin. Tech. of the Comm. on Fin. Services*, 117 Cong. (2022) https://democrats-financialservices.house.gov/events/eventsingle.aspx?EventID=409260 [https://perma.cc/TQK9-7N8T].

120. Protecting Consumers From Payment Scams Act, *supra* note 118.

121. FACILITATING FRAUD , *supra* note 19, at 9.

122. For the legal definition of error, see 15 U.S.C. 1693f(f); 12 C.F.R. 1005.11(a)(1).

123. 12 C.F.R. 1005.11(c)(1)-(2).

circumstances);[124] report the results of the investigation to the consumer within three business days of completing the investigation;[125] and correct the error within one business day after determining that an error has occurred.[126]

EFTA defines an "error":

(1) an **unauthorized** electronic fund transfer;
(2) an **incorrect** electronic fund transfer from or to the consumer's account;
(3) the omission from a periodic statement of an electronic fund transfer affecting the consumer's account which should have been included;
(4) a computational error by the financial institution;
(5) the consumer's receipt of an incorrect amount of money from an electronic terminal;
(6) a consumer's request for additional information or clarification concerning an electronic fund transfer or any documentation required by this subchapter; or
(7) **any other error described in regulations of the Bureau**.[127]

Regulation E's definition of an error is very close to the statutory definition,[128] and only one provision of the regulations is the result of the Bureau using its statutory authority under EFTA to designate something else as an error.[129] The commentary provides that financial institutions are required to comply with the error resolution procedures "when a consumer reports the loss or theft of an access device if the consumer also alleges possible unauthorized use as a consequence of the loss or theft."[130] But the regulations and comments leave unclear whether financial institutions have to follow the error resolution procedures when the consumer is defrauded into making payments.

Neither the statute nor the regulation have changed in any meaningful way since first adopted, other than transfer of regulatory authority

---

124. The time can be extended to forty-five days if the institution is "unable to complete its investigation within 10 business days" and provisionally credits the consumer's account within ten days of receiving the error notice. 12 C.F.R. 1005.11(c); 12 C.F.R. 1005.11(c)(2). This time period is changed to twenty days with a possible 90-day extension for errors that are initiated out of state or involve a point-of-sale debit card transaction. 12 C.F.R. 1005.11(c)(3).

125. 12 C.F.R. 1005.11(c)(2)(iv).

126. 12 C.F.R. § 1005.11(c)(2)(iii) (2023).

127. 15 U.S.C. § 1693f(f) (2023) (emphasis added).

128. 12 C.F.R § 1005.11(a).

129. 12 C.F.R. § 1005.11(a)(1)(vi) (2023) (defining an error as "[a]n electronic fund transfer not identified in accordance with § 1005.9 [ATM receipts and periodic statements] or § 1005.10(a) [pre-authorized transfers]").

130. 12 C.F.R §1005.11 (Supp. 1).

from the Federal Reserve Board to the Consumer Financial Protection Bureau under the Dodd-Frank Wall Street Reform and Consumer Protection Act, adopted in July 2010.[131] The statute and regulation provide two legislative/regulatory routes for designating payments initiated by an authorized party who has been manipulated, defrauded, or conned into sending a payment as payments made in "error" under the EFTA. First, the CFPB could use its authority to define additional categories of errors under EFTA.[132] Second, Congress or the CFPB could designate or clarify that payments made in this way are "incorrect" and therefore subject to the error resolution processes.[133]

Consumer advocates have argued that payments made by consumers induced by fraud or a scam are indeed payments made in error.[134] This is particularly true for payments that involve impersonation.[135] If a consumer is told that they are sending funds to their bank, their utility company, the IRS, their grandchild, or an imposter using a fake name, but in reality the money is going to someone else, that is arguably an error. There is an even stronger case for error where a fraudster is able to impersonate the consumer's bank and link the consumer's cell phone number to the scammer's account in order to perpetrate a me-to-me scam. The senators who have engaged with the CFPB on this issue agreed, writing to Rohit Chopra, Director of the CFPB:

> The CFPB could clarify that, in certain circumstances, a payment is an 'error' when a consumer is defrauded into initiating a transfer to a scammer. Indeed, the EFTA already provides the CFPB with authority to prescribe additional categories of 'error'

131. *See* Pub. L. No. 95-630, § 908, 92 Stat. 3641 (1978) (codified as amended at 15 U.S.C. § 1693f); amended Pub. L. 111-203, § 1084, 124 Stat. 1376, 2081 (July 21, 2010). The regulation was previously 12 C.F.R. 205.11. Although the wording has changed some, the essence of the regulation has not. 45 Fed. Reg. 8248, 8265 (Feb. 6, 1980); Technical Amendments and Update to Official Staff Commentary, 48 Fed. Reg. 14880, 14881 (April 6, 1983); Final Rule and Update on Official Staff Commentary, 49 Fed. Reg. 40794, 40798 (May 2, 1996); 63 Fed. Reg. 52115, 52118 (Sept. 29, 1998).

132. *See* 15 U.S.C. § 1693f(f)(7) (2023).

133. 15 U.S.C. § 1693f(f)(2); 12 C.F.R. § 1005.11(a)(1)(ii).

134. Andrew Ackerman, *CFPB to Push Banks to Cover More Payment Services Scams*, WALL ST. J. (July 19, 2022), https://www.wsj.com/articles/consumer-bureau-to-push-banks-to-refund-more-victims-of-scams-on-zelle-other-services-11658235601 [https://perma.cc/9A4H-27MA] (quoting Lauren Saunders, Assoc. Dir., Nat. Consumer L. Ctr.) ("If a bank mistakenly links your cellphone number to a scammer's account, that's an error that should be corrected and you should be able to get your money back."); Comment by Mark E. Budnitz, Bobby Lee Cook Professor of Law Emeritus, Georgia State Univ. College of Law, CFPB Docket Number CFPB-2021-0017, Comment ID CFPB-2021-0017-0095 (available at regulations.gov).

135. For information about imposter scams, *See How to Avoid Imposter Scams*, FED. TRADE COMM'N., https://consumer.ftc.gov/features/imposter-scams [https://perma.cc/V5PW-TEL6] (last visited Sept. 18, 2023).

> transactions that the financial institution – rather than the consumer – should be responsible for correcting.[136]

The CFPB could also choose to designate payments induced by fraud or a scam as "incorrect" payments. A payment that is "incorrect" is considered a payment in error under EFTA and Regulation E, entitling the consumer to all of the rights involved when a payment is made in error.[137] The problem is that the statute and its companion regulation do not give a definition of "incorrect." Even the legislative history of EFTA is unhelpful in this regard, although at least one witness at a 1977 hearing on what became EFTA urged Congress to define the word "incorrect."[138] This means that in order to designate these types of payments as incorrect, the CFPB would have to engage in textual interpretation of the word incorrect. In doing so, an argument could be made that a payment induced by fraud is an incorrect payment as that word is commonly defined: inaccurate, wrong, improper, or erroneous.[139]

Thus, the CFPB could, without further congressional action, issue a regulation defining an additional category of error, or clarify the meaning of "incorrect."

Of course, Congress could also address the issue directly. One approach is the one taken in the "Protecting Consumers From Payment Scams Act," circulated but not introduced during the 117th Congress, 2nd session. That bill addressed "errors" and "incorrect payments" in two places. First, the bill proposed amending the subsection designating incorrect payments as payments made in error as follows (with added language in italics):

> (2) an incorrect electronic fund transfer from or to the consumer's account *including an error made by a consumer*;[140]

---

136. Letter from U.S. Sens. to Rohit Chopra, *supra* note 102.

137. 15 U.S.C. § 1693f(f)(2); 12 C.F.R. § 1005.11(a)(1)(ii).

138. *Electronic Fund Transfer Act: Hearings on S. 2065 Before the Subcomm. on Consumer Aff. of the S. Comm. on Banking, Hous., and Urban Aff.*, 95th Cong. 90 (1977) (Statement of James L. Brown, Acting Dir., Center for Consumer Affairs, University of Wisconsin) ("Additionally, I would recommend defining what constitutes an "incorrect" transfer as referred to in subsection (e)(2). Presumably. this would encompass transfers erroneous in amount. However, it could be construed to include situations where the consumer enterers an unintended amount and such amount is actually transferred. I believe that such definitions should be created in the statute rather than relying upon the board to follow such an unclear direction.")

139. *Inaccurate*, DICTIONARY.COM, https://www.dictionary.com/browse/incorrect [https://perma.cc/S9SH-NN5K] (last visited Sept. 18, 2023).

140. Protecting Consumers From Payment Scams Act, *supra* note 118, at § 2(b)(1).

Second, the draft bill expanded the definition of unauthorized transactions to include those transactions that are fraudulently induced.[141] Since unauthorized transfers are a specifically listed type of error, any change to EFTA that makes fraudulently induced transactions "unauthorized" would also provide consumers with the protections for a payment made in error.

As of the writing of this Article, the CFPB has not taken action to expand the categories of error under its statutory authority or to clarify the meaning of "incorrect." The draft bill, as stated, was pulled from the House Financial Services Committee's website after the seating of the 118th Congress.[142]

3. Liability shifting once EFTA and Regulation E are updated

If EFTA were updated or clarified to protect consumers when they are fraudulently induced into sending money to a fraudster, the consumer would notify their own bank that they had been a victim of fraud. The bank would have to recognize the payment as unauthorized, in error, or incorrect. The consumer's bank would be responsible in the first instance for recrediting the consumer's account. An appropriate liability scheme would ultimately shift that liability from the consumer's bank to the bank that holds the account of the fraudster or the fraudster's agent (known as a money mule, and described below). This bank is called the "receiving bank" because it "receives" the payment into the account of the fraudster. If the fraudster cannot be found, the receiving bank is the next most appropriate party to bear the loss.

The discussion draft of the "Protecting Consumers From Payment Scams Act" includes a provision shifting liability to the receiving bank that holds the fraudster's account.[143] Liability shifting to the receiving bank can also happen through the private rules that govern payment systems such as Zelle. This is an important step for open loop payment

141. *Id.*

142. The discussion of the draft bill is still available on the website of the House of Representatives. *See Protecting Consumers From Payment Scams Act: Hearing on H.R. __ Before the H. Comm. on Financial Services*, 117th Cong. (2022), https://democrats-financialservices.house.gov/events/eventsingle.aspx?EventID=409260 [https://perma.cc/JML5-HNP8].

143. Protecting Consumers From Payment Scams Act, *supra* note 118, §2(f) ("If a consumer's financial institution credits the consumer's account for an electronic fund transfer that was initiated by the consumer but was fraudulently induced, the financial institution that received the transfer shall be liable to the consumer's financial institution for the amount of the credit.")

systems, which process payments for customers at different banks.[144] It is not as important for closed systems such as Venmo, PayPal and Cash App because the company holds the accounts at both ends.[145]

Imposing greater responsibilities on the receiving bank ensures that the banks that let fraudsters into the banking system incur the liability if their customer disappears with ill-gotten gains. Banks have the legal responsibility to know their customers and to prevent unlawful use of their accounts (as discussed in the next Section of this Article). They have tools they can use to prevent fraudulent accounts from being opened in the first place and to detect improper use of accounts. Yet, without liability when they fall short on these obligations, receiving banks do not have sufficient incentive to invest effort, resources, and innovative creativity into fraud prevention efforts. Most fraud prevention efforts are focused on account takeover (i.e., hacking into the consumer's account), where banks bear liability for unauthorized use. Far less attention focuses on the role of the receiving bank. That needs to change.

B. *Solutions involving Bank Secrecy Act/Anti-Money Laundering Requirements and better fraud detection*

"If a bank permits a scammer or fraudster onto the platform, then that bank should naturally bear some responsibility when its own customer uses a bank-provided payment service to rip off others – rather than telling customers that it is their fault for being victimized"[146]

The shift in liability to the fraudster's bank discussed in Part A of this Article would incentivize banks to refuse to bank fraudsters. But another way to incentivize banks to protect the banking system and consumers from fraudsters involves "know your customer" obligations imposed on banks under the Bank Secrecy Act and related laws. The system for detecting, reporting, and thwarting fraud and other crimes in and through the U.S. financial system is generally referred to as "BSA/AML." "BSA" references the "Bank Secrecy Act," "AML" refers to "Anti-Money Laundering," and "BSA/AML" is shorthand for "a series of laws and

144. *What is an Open Loop Payment System?*, MODERN TREASURY, https://www.moderntreasury.com/learn/open-loop-payment-system [https://perma.cc/H7SQ-DF7T] (last visited Jan. 20, 2024).

145. *Id.* It is important to note, though, that consumers can face risks when they store money in Venmo and other closed systems because these apps are not covered by deposit insurance. Ken Sweet, *Money Stored in Venmo and Other Payments Apps Could Be Vulnerable, Financial Watchdog Warns*, ASSOCIATED PRESS (June 2, 2023, 4:54 AM), https://apnews.com/article/venmo-paypal-cashapp-p2p-payments-deposit-insurance-f89eba2486a383160b9343e2e4e60b3f [https://perma.cc/F6DT-79KW].

146. Letter from U.S. Sens. to Rohit Chopra, *supra* note 102.

regulations enacted in the U.S. to combat money laundering and the financing of terrorism."[147] This Section analyzes the current BSA/AML legal regime and changes being considered to that regime that would improve robust monitoring systems to detect fraudsters and keep fraudsters out of the banking system. These changes, suggested in Section B(2) of this Article[148] would help financial institutions root out P2P payments fraud, and serve to protect their customers.

In a perfect "to catch a thief" world, when someone became the victim of a P2P payments scam, that victim would complain to their bank, which would then contact the fraudster's bank that received the payment. Also in a perfect world, detection would happen quickly. The fraudster's bank would be required to refund payments to the victim's bank, as discussed in Section A of this Article, which would refund the victim. The fraudster's bank would be able to recoup some losses from the fraudster's account, and any losses unrecoverable from the fraudster would be borne by the fraudster's bank (who gave the fraudster the key to the door to begin with).

As fraud victims' banks made credible fraud complaints with the fraudster's bank, the fraudster's bank would become suspicious. It would report the fraud to the proper authorities *and* have some methodology for reporting the fraud to other financial institutions. That bank would then freeze and eventually close the accounts of the fraudster, thereby cutting off the fraudster's access to the system through *one* of many possible doors. In the meantime, law enforcement, perhaps with the help of the fraudster's financial institution, would work on identifying the true owner of the account used to commit fraud. After all, fraudsters do not usually receive money directly into accounts in their own name, or else it would be very simple to find them and pass losses back to them. Instead, fraudsters either use accounts newly opened with stolen or synthetic identities, or use they use money mules (discussed below) who launder the funds, or they hide behind one or more businesses and shell corporations.[149] Eventually, the fraudster and their known associates and

147. *Bank Secrecy Act/Anti-Money Laundering (BSA/AML)*, FEDERAL DEPOSIT INSURANCE CORPORATION https://www.fdic.gov/resources/bankers/bank-secrecy-act/ [https://perma.cc/AR2T-8GDH] (last visited Sept. 15, 2023).

148. *See infra* Section B (2).

149. LEXISNEXIS RISK SOLUTIONS, UNCOVERING SYNTHETIC IDENTITY FRAUD 1–2 (2021), https://risk.lexisnexis.com/insights-resources/article/synthetic-identity-fraud [https://perma.cc/VU8H-7WGQ]; *Money Mules*, FBI, https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/money-mules [https://perma.cc/RC9J-UV92] (last visited Jan. 20, 2024); *see also* FIN. CRIMES ENF'T NETWORK, *supra* note 21; *Combating Illicit Financing by Anonymous Shell Companies Before the Senate Banking, Hous., and. Urb. Affs. Comm.*, 116th Cong. (2019) (testimony of Steven M. D'Antuono, Acting Deputy Assistant Director, Criminal Investigative Division,

affiliates would be treated as one and the same. The fraudster (and their known associates and affiliates) would go looking for another place to bank, but any new bank approached by the fraudster and company would know from information gleaned from the fraudster's prior bank or from law enforcement that the account applicant was a fraudster. The new bank would also be able to check a central location for names affiliated with the fraudster, such as businesses controlled or owned by the fraudster, or accomplices of the fraudster. The fraudster and the fraudster's associates and affiliates would be unable to open another door and future victims would not materialize. Or, at least, if a new account was opened, it would be monitored closely for indicia of fraud.

The Bank Secrecy Act was first adopted in 1970.[150] Responding to the September 11, 2001 attacks, Congress adopted the USA PATRIOT Act, which imposed further requirements on financial institutions.[151] These requirements have continued to evolve in order to keep the United States in conformity with international anti-money laundering standards set by the Financial Action Task Force ("FATF")[152], and most recently through the Anti-Money Laundering Act of 2020.[153] The Financial Crimes Enforcement Network ("FinCEN") promulgates and enforces the Bank Secrecy Act regulations.[154] Examination for financial institution

---

Federal Bureau of Investigation), https://www.fbi.gov/news/testimony/combating-illicit-financing-by-anonymous-shell-companies [https://perma.cc/93AR-KUBD].

150. Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1122 (1970).

151. Pub. L. No. 107-56, 115 Stat. 273 (2001). Discussion of bank accounts and the 9/11 attacks can be found in the 9/11 Commission's final report: NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, *The Attack Looms*, *in* 9-11 COMMISSION REPORT 215, 237 (2004) ("The hijackers made extensive use of banks in the United States, choosing both branches of major international banks and smaller regional banks. All of the hijackers opened accounts in their own name, and used passports and other identification documents that appeared valid on their face. Contrary to numerous published reports, there is no evidence the hijackers ever used false Social Security numbers to open any bank accounts. While the hijackers were not experts on the use of the U.S. financial system, nothing they did would have led the banks to suspect criminal behavior, let alone a terrorist plot to commit mass murder.") https://9-11commission.gov/report/ [https://perma.cc/62NK-CY4Y].

152. For the latest update to the FATF standards, see FIN. ACTION TASK FORCE, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION THE FATF RECOMMENDATIONS (2023), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf [https://perma.cc/MVW2-643H].

153. Anti-Money Laundering Act of 2020, Pub. L. No. 116-283, §§ 6101-6511, 2020 U.S.C.C.A.N. 134 Stat. 3388, 4549 (Jan. 1, 2021).

154. FinCEN has delegated authority from the Secretary of the Treasury Department, and is authorized to impose anti-money laundering program requirements on financial institutions, and require financial institutions to maintain procedures to ensure compliance with Bank Secrecy Act laws and regulations. Treas. Deleg. Order 180-01 (July 1, 2014), 31 U.S.C. § 5318(a)(2), (n)(4)(B) (2018). *See also* Financial Crimes Enforcement Network, Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29398, 29399 (May 11, 2016). "The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic

compliance with BSA/AML requirements is delegated to and carried out by the various prudential regulators, including the Office of the Comptroller of the Currency (OCC), the National Credit Union Administration (NCUA), the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System.[155]

The BSA/AML regime was augmented by the Anti-Money Laundering Act of 2020[156]—a statute that has been called "the most consequential anti-money laundering legislation passed by Congress in decades."[157] The statute specifically seeks to strengthen FinCEN[158] and calls for "modernizing the anti-money laundering and countering the financing of terrorism system" by, among other things, requiring that FinCEN review and revise as appropriate its BSA regulations and guidance, including reporting requirements.[159] In December, 2021, in response to this mandate, FinCEN issued a Request for Information and Comment, soliciting comments on "ways to streamline, modernize, and update the anti-money laundering and countering the financing terrorism (AML/CFT) regime of the United States."[160] On July 20, 2022, Congress increased FinCEN's budget by 31%—a massive increase to facilitate compliance with the Anti-Money Laundering Act of 2020.[161]

It has long been recognized that the BSA/AML system has a key role to play in protecting victims and potential victims of payments fraud. In fact, when FinCEN proposed a new Customer Due Diligence Rule (CDD) in 2014,[162] the Federal Trade Commission (FTC) filed a comment on the value of the beneficial ownership portion of the proposed rule (discussed

use of financial authorities and the collection, analysis, and dissemination of financial intelligence." *Mission Statement*, FIN. CRIM. ENF'T NETWORK, https://www.fincen.gov/about/mission [https://perma.cc/E64Z-9YAK] (last visited Jan. 20, 2024).

155. *See* 12 C.F.R. § 21 (2023); 12 C.F.R. § 748 (2023); 12 C.F.R. § 326 (2023); *see also Bank Secrecy Act Resources*, NAT'L CREDIT UNION ADMIN. (Dec. 10, 2021), https://ncua.gov/regulation-supervision/regulatory-compliance-resources/bank-secrecy-act-resources [https://perma.cc/M8CY-7F9C].

156. *See* Anti-Money Laundering Act of 2020, Pub. L. No. 116-283, §§ 6101-6511, 2020 U.S.C.C.A.N. 134 Stat. 3388, 4549 (Jan. 1, 2021).

157. Andres Fernandez & Eddie A. Jauregui, *Key Provisions of the Anti-Money Laundering Act of 2020*, HOLLAND & KNIGHT (Jan. 13, 2021), https://www.hklaw.com/en/insights/publications/2021/01/key-provisions-of-the-anti-money-laundering-act-of-2020 [https://perma.cc/FC7H-7KA9].

158. *See* Anti-Money Laundering Act of 2020, Pub. L. No. 116-283, §§ 6101-6511, 2020 U.S.C.C.A.N. 134 Stat. 3388, 4566 (Jan. 1, 2021).

159. Anti-Money Laundering Act of 2020, Pub. L. No. 116-283, Title LXII § 6216, 134 Stat. 4582-83 (Jan. 1 2021).

160. Request for Information and Comment, 86 Fed. Reg. 71201 (Dec. 15, 2021) (to be codified at 31 C.F.R. ch. X).

161. Erica Hanichak, *House Passes Bill to Boost Budget of Nation's Financial Crime Fighters*, FIN. ACCOUNTABILITY & CORP. TRANSPARENCY COAL. (July 20, 2022), https://thefactcoalition.org/house-passes-bill-to-boost-budget-of-nations-financial-crime-fighters/ [perma.cc/29JX-4XQG].

162. Notice of Proposed Rulemaking Customer Due Diligence Requirements for Financial Institutions, 79 Fed. Reg. 45151 (Aug. 4, 2014) (to be codified at 31 C.F.R. pts. 1010, 1020, 1023, 1024, 1026).

below) to "track[ing] down those perpetrating fraud against consumers."[163] The most recent National Money Laundering Risk Assessment (2022) recognizes that "[f]raud, both in the private sector and in government benefits and payments, continues to be the largest driver of money laundering activity in terms of the scope of activity and magnitude of illicit proceeds, generating billions of dollars annually."[164] Fraud, and particularly fraud that is "internet-enabled" or committed through cybercrime, is one of eight national priorities for anti-money laundering and countering the financing of terrorism efforts announced in 2021.[165] Although the national priorities address all kinds of fraud, including health, securities, and tax fraud, consumer fraud schemes that are "internet enabled," such as "romance scams, synthetic identity fraud, and other forms of identity theft" are called out in particular.[166] One of the articulated purposes of the Anti-Money Laundering Act of 2020 is to assess the fraud risks to financial institutions in order to protect the U.S. financial system from criminal abuse.[167]

The BSA/AML system's potential to protect consumers from payments fraud by protecting the financial system itself from fraudsters has never been fully realized, in part because the common interests of the consumer protection community, financial institutions, and BSA/AML regulators have never been fully explored. But because of the Anti-Money Laundering Act of 2020[168] and FinCEN's resulting systemic review, the BSA/AML system is poised at this very moment to make some significant changes that will increase the ability of banks and financial institutions to detect, report, and prevent payments fraud—including fraud through P2P payment systems.[169]

---

163. *Proposed FinCEN Rule Should Help FTC Track Down Perpetrators of Fraud*, FED. TRADE COMM'N (Oct. 7, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/10/proposed-fincen-rule-should-help-ftc-track-down-perpetrators-fraud [perma.cc/5A2J-YZWM]; Fed. Trade Comm'n. Staff, Comment on Financial Crimes Enforcement Network's Proposed Customer Due Diligence Rule for Financial Institutions (Oct. 3, 2014) (Docket Number FINCEN-2014-0001; RIN 1506-AB25) https://www.ftc.gov/legal-library/browse/advocacy-filings/ftc-staff-comment-financial-crimes-enforcement-networks-proposed-customer-due-diligence-rule [perma.cc/9N66-PHK6].

164. U.S. DEP'T OF THE TREASURY, NATIONAL MONEY LAUNDERING RISK ASSESSMENT 5 (Feb. 2022), https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf [perma.cc/P5Z9-SQBH]. *See, also,* FIN. CRIMES ENF'T. NETWORK, ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM NATIONAL PRIORITIES 8 (June 30, 2021), https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf [perma.cc/KM8M-JKFX].

165. FIN. CRIMES ENF'T. NETWORK, *supra* note 164, at 8.

166. FIN. CRIMES ENF'T. NETWORK, *supra* note 164, at 8.

167. Pub. L. No. 116–283, § 6101, 134 Stat. 4547 (2021) (codified at 31 U.S.C. 5311(4)).

168. Pub. L. No. 116–283, §§ 6101–6511, 134 Stat. 4547 (2021).

169. For general discussions about Financial Crime committed in real time payments, see Grant Vickers, *Using AI to Combat Financial Crime in Real-Time Payments*, PAYMENTSJOURNAL (Apr. 3, 2023), https://www.paymentsjournal.com/using-ai-to-combat-financial-crime-in-real-time-payments/ [https://perma.cc/5BTM-MDW8].

1. The Current BSA/AML Regime

It is important to start by noting that banks are permitted to set their own risk tolerances for customers. This means that banks are not required or even encouraged to refuse to open accounts for certain types of customers or certain industries but must decide what types of customers fit into the bank's risk tolerance. As put by the prudential regulators: "Banks determine the levels and types of risks that they will assume. Banks that operate in compliance with applicable law, properly manage customer relationships and effectively mitigate risks by implementing controls commensurate with those risks are neither prohibited nor discouraged from providing banking services."[170] "As a general matter, the agencies do not direct banks to open, close, or maintain specific accounts."[171]

Although the law does not prevent banks from doing business with anyone, BSA/AML laws require that banks "know their customer" (through specific provisions to be discussed below), and file reports of certain types of activity. The higher the risk a customer poses to the bank, the more likely the bank is to need extensive BSA/AML customer monitoring. Thus, banks might choose not to bank an individual or company based on the risks the customer might pose for the bank, but they are not prohibited from doing business with a particular group or class of customers.

In its current form, the Bank Secrecy Act and its implementing regulations require financial institutions to collect information at account opening and detect certain activity during the course of the bank/customer relationship. Overall, the bank is required to have an effective, risk-based anti-money laundering and Bank Secrecy Act compliance program,[172] and failure to have such a program designed to

170. Joint Statement, Board of Governors of the Federal Reserve System, FDIC, FinCEN, NCUA, OCC, Joint Statement on Risk-Focused Bank Secrecy Act/Anti-Money Laundering Supervision 2 (July 22, 2019), https://www.fincen.gov/news/news-releases/joint-statement-risk-focused-bank-secrecy-actanti-money-laundering-supervision [https://perma.cc/Q5TV-EFZW].

171. Joint Statement, Board of Governors of the Federal Reserve System, FDIC, FinCEN, NCUA, OCC, Joint Statement on Risk-Focused Bank Secrecy Act/Anti-Money Laundering Supervision 2 (July 6, 2022), https://www.occ.gov/news-issuances/bulletins/2022/bulletin-2022-18a.pdf [https://perma.cc/EF6D-3ZKS]. *See also* FFIEC BSA/AML, *Introduction*, *in* EXAMINATION MANUAL (Nov. 2021), https://bsaaml.ffiec.gov/manual [https://perma.cc/87JR-KMY9].

172. 12 U.S.C. § 1818(s); 12 U.S.C. § 1786(q); 31 U.S.C. § 5318(h); 31 C.F.R. § 1020.210; 12 C.F.R. § 21.21; Board of Governors of the Federal Reserve System, FDIC, FinCEN, NCUA, OCC, *supra* note 170. *See Bank Secrecy Act (BSA) & Related Regulations*, OFF. COMPTROLLER CURRENCY (last visited Sept. 19, 2023) ("This regulation requires every national bank and savings association to have a written, board approved program that is reasonably designed to assure and monitor compliance with the BSA. The program must, at a minimum:

1. provide for a system of internal controls to assure ongoing compliance;
2. provide for independent testing for compliance;

carry out the bank's BSA obligations can get the bank in a lot of regulatory trouble.[173]

Financial institution obligations under this regime are sometimes collectively referred to as "Customer Due Diligence," or "CDD." CDD involves:

1. Customer identification and verification,
2. Beneficial ownership identification and verification,
3. Understanding the nature and purpose of customer relationships to develop a customer risk profile, and
4. Ongoing monitoring for reporting suspicious transactions and, on a risk basis, maintaining and updating customer information.[174]

These obligations can be roughly divided into three groups—obligations at account opening (sometimes called customer onboarding); obligations to monitor the account during the life of the account; and obligations to report certain types of activities. Each of these phases in the bank customer relationship will be discussed separately.

a. *Customer Onboarding/Account Opening*

i. Customer Identification and verification

When a bank opens an account for a customer, the bank is required to properly identify the party opening the account. The bank must not open an account in the name of an alias, for an individual or customer other than the person actually opening the account, or for someone prohibited from having an account, such as an individual subject to

---

3. designate an individual responsible for coordinating and monitoring day-to-day compliance; and
4. provide training for appropriate personnel. In addition, the implementing regulation for section 326 of the PATRIOT Act requires that every bank adopt a customer identification program as part of its BSA compliance program.").

https://www.occ.treas.gov/topics/supervision-and-examination/bsa/bsa-related-regulations/index-bsa-and-related-regulations.html [https://perma.cc/XN3N-MGGX]; *see also Bank Secrecy Act (BSA)*, OFF. COMPTROLLER CURRENCY (last visited Sept. 19, 2023) https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html/ [https://perma.cc/QW9B-TNQT].

173. *Enforcement Actions*, FIN. CRIMES ENF'T NETWORK (last visited Sept. 19, 2023) https://www.fincen.gov/news-room/enforcement-actions [https://perma.cc/YEJ4-ZF4X].

174. Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29398 (2016) (amended by Customer Identification Programs, Anti-Money Laundering Programs, and Beneficial Ownership Requirements for Banks Lacking a Federal Function Regulator, 85 Fed. Reg. 57129, 57137-38 (2020)) (codified as amended at 31 C.F.R. § 1020.210 (2024)).

sanctions.[175] These requirements are part of a bank's customer due diligence, or CDD, requirements.[176]

One major part of this obligation can be found in the "customer identification program" (or "CIP") rule,[177] which sets minimum requirements at account opening and also mandates that banks have their own rules that they strictly adhere to. Under the customer identification rules, the bank must follow minimum requirements, including obtaining an account applicant's name, date of birth (individual), address, and ID number, such as social security or taxpayer identification number.[178] Additionally, the bank must have the following procedures in place:

- "[R]isk based procedures for verifying the identity of each customer to the extent reasonable and practicable. The procedures must enable the bank to form a reasonable belief that it knows the true identity of each customer. These procedures must be based on the bank's assessment of the relevant risks, including those presented by the various types of accounts maintained by the bank, the various methods of opening accounts provided by the bank, the various types of identifying information available, and the bank's size, location, and customer base."[179]
- The procedures must allow for verifying the identity of the customer "within a reasonable time after the account is opened."[180]
- The procedures must designate "when the bank will use documents, non-documentary methods, or a combination of both" to verify the customer's identity, what documents will be used (and there is a list of documents the bank may include), and what non-documentary methods the bank will use.[181]

175. Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29398 (May 11, 2016) (to be codified at 31 C.F.R. pts. 1010, 1020, 1024, 1026; 31 C.F.R. § 1020.210.) Generally, any individual or company listed on the "Specially Designated Nationals and Block Persons List (SDN)," maintained by the Office of Foreign Asset Control (OFAC), list cannot be banked. The SDN list can be accessed at *Specially Designated Nationals and Block Persons List (SDN) Human Readable Lists*, U.S. DEP'T TREASURY, https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists [https://perma.cc/7Q6E-Y85G] (last accessed Jan. 20, 2024).

176. Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29398 (May 11, 2016) (to be codified at 31 C.F.R. pts. 1010, 1020, 1024, 1026; 31 C.F.R. § 1020.210.

177. 31 C.F.R. § 1020.220 (2020); 31 U.S.C. § 5318.

178. 31 C.F.R. § 1020.220 (a)(2)(i) (2020).

179. *Id.* § 1020.220(a)(2) (2020).

180. *Id.* § 1020.220(a)(2)(ii) (2020).

181. *Id.*

- The procedures must designate when, based on the bank's risk assessment, the bank will "obtain information about individuals with authority or control over such account"[182] if the customer's true identity cannot be verified using the basic methods.[183]
- The procedures must indicate what the bank will do if the bank "cannot form a reasonable belief that it knows the true identity of a customer," including when the bank will refuse to open an account; when and under what terms the bank will allow the customer to use the account while verification is pending; when attempts to verify will be deemed to have failed and the account will be closed; and when the bank should file a suspicious activity report (discussed below).[184]
- The procedures must have rules for "making and maintaining a record of all information" from the verification process (with minimum records requirements and a five-year retention rule set out in the regulation).[185]
- The procedures must include how customers will be adequately notified that the bank is requesting information from them.[186]
- The procedures must indicate when the bank will rely on CIP performed by another institution.[187]
- Finally, the procedures must indicate how the bank will screen its new accounts for compliance with anti-terrorist or other sanctions lists.[188]

ii. Determining Beneficial Ownership

Proper identification of the customer includes clearly identifying who actually stands behind an account held in the name of a business. In that case, the individuals who own or control the legal entity are referred to as the entity's "beneficial owners."[189] In the 2016 mutual evaluation of

182. *Id.* § 1020.220(a)(2)(ii)(C) (2020).
183. *Id.*
184. *Id.* § 1020.220(a)(2)(iii) (2020).
185. *Id.* § 1020.220(a)(3) (2020).
186. *Id.* § 1020.220(a)(5) (2020).
187. *Id.* § 1020.220(a)(6) (2020).
188. *Id.* § 1020.220(a)(4) (2020); *see generally* 31 C.F.R. § 500, *et. seq*.
189. Financial Crimes Enforcement Network, Customer Due Diligence Requirements for Financial Institutions, Final Rule, 81 Fed. Reg. 29398 (May 11, 2016); FIN. ACTION TASK FORCE, *supra* note 152, at 121 (which defines beneficial owner as: "Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction

the U.S.'s anti-money laundering and counter-terrorist measures, the Financial Action Task Force found that lack of beneficial ownership requirements in the U.S.'s BSA/AML system was a "fundamental gap" in the U.S.'s measures.[190] FinCEN had previously issued guidance on the matter, followed by a rule adopted in 2016.[191] The 2016 rule required all financial institutions to "identify and verify the identity of the beneficial owners of all legal entity customers . . . at the time a new account is opened" and as part of their ongoing monitoring of customer accounts.[192] The rule defined "beneficial owner" based on direct or indirect ownership of the entity, or ability to control, manage or direct the legal entity.[193] The process allowed banks to obtain the information from customers at account opening and rely on that information unless the bank had "knowledge of facts that would reasonably call into question the reliability of the information."[194]

In September 2022, a new rule strengthened the U.S. beneficial ownership regime immensely. The rule requires most companies registered to do business in the United States (including in all States or Tribal jurisdictions) to report information about the company's beneficial owners, including changes in ownership, to FinCEN.[195] The rule defines a beneficial owner as "any individual who, directly or indirectly, either exercises substantial control over such reporting company or owns or controls at least 25 percent of the ownership interests of such company."[196] It goes on to say that an individual can exercise substantial control in a number ways, including by serving as a senior officer, or influencing important decisions made by the company.[197] This new rule closes a "major gap" in

---

is being conducted. It also includes those natural persons who exercise ultimate effective control over a legal person or arrangement. Only a natural person can be an ultimate beneficial owner, and more than one natural person can be the ultimate beneficial owner of a given legal person or arrangement.").

190. FIN. ACTION TASK FORCE, ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING MEASURES: UNITED STATES: MUTUAL EVALUATION REPORT 4, 5, 10, 18, 20, 37 (2016), https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf [https://perma.cc/KB8E-WXCG].

191. FIN. CRIMES ENF'T. NETWORK ET AL., FIN -2010-G001, GUIDANCE ON OBTAINING AND RETAINING BENEFICIAL OWNERSHIP INFORMATION, (Mar. 5, 2010); Customer Due Diligence Requirements for Financial Institutions Final Rule, 81 Fed. Reg. 29398 (May 11, 2016).

192. 81 Fed. Reg. 29398; 31 C.F.R. § 1010.230(b)(1); 31 C.F.R. § 1020.210(a)(v)(B); 31 C.F.R. 1020.210(b)(2)(v)(B).(b)(5)(ii).

193. 81 Fed. Reg. 29398, 29451-52; 31 C.F.R. § 1010.230(d).

194. 81 Fed. Reg. 29398.

195. Corporate Transparency Act, Pub. L. 166-283, Title LXIV, 134 Stat. 3338, 4605-06 (Jan. 1, 2021); Fin. Crimes Enf't. Network et al., Beneficial Ownership Information Reporting Requirements Final Rule, 87 Fed. Reg. 59498 (Sept. 30, 2022); 31 C.F.R. § 1010.380.

196. Ownership Information Reporting Requirements Final Rule, 87 Fed. Reg. 59498, 59525 (Sept. 30, 2022); 31 C.F.R. 1010.380(d).

197. 87 Fed. Reg. 59498, 59525 (Sept. 30, 2022); 31 C.F.R. 1010.380(d).

the ability of the U.S. to detect and prevent criminal activity, including fraud, money laundering, and the financing of terrorism.[198] However, it remains to be seen who will be able to access this information.

iii. Determining whether to open an account

Assuming a bank has correctly identified the customer, the next step is to decide if the bank will open an account for that customer. Generally, a bank cannot do business with any individual or company listed on the "Specially Designated Nationals and Blocked Persons List (SDN)", maintained by the Office of Foreign Asset Control (OFAC).[199] Other than this list of forbidden accounts, the decision whether to bank a customer or not is based on the financial institution's risk profile.

iv. Level Setting for Suspicious Activity Reporting

Once the bank decides to open an account, it is required to create a customer risk profile, which is then "used to develop a baseline against which customer activity is assessed for suspicious activity reporting."[200]

b. *Account Monitoring and Reporting*

Once an account has been opened, the bank must have effective due diligence systems and customer monitoring programs.[201] As part of these programs, the bank is supposed to screen the account for any activity that seems suspicious or out of character for the account given the account history, and the purpose for which the account was purportedly opened, and for large cash transactions.[202]

---

198. U.S. DEP'T. OF THE TREASURY, *supra* note 164, at 36.

199. *Specially Designated Nationals and Block Persons List (SDN) Human Readable Lists*, *supra* note 175.

200. Financial Crimes Enforcement Network, Customer Due Diligence Requirements for Financial Institutions, Final Rule, 81 Fed. Reg. 29398, 29398 (May 11, 2016); 31 C.F.R. 1020.210(b)(i); Board of Governors of the Fed. Res. Sys., FDIC, FinCEN, NCUA, OCC, Joint Statement on Risk-Focused Bank Secrecy Act/Anti-Money Laundering Supervision (July 6, 2022), https://www.occ.gov/news-issuances/bulletins/2022/bulletin-2022-18a.pdf [https://perma.cc/2DP7-FJJK].

201. *See* Financial Crimes Enforcement Network, Customer Due Diligence Requirements for Financial Institutions, Final Rule, 81 Fed. Reg. 29398 (May 11, 2016); 31 C.F.R. § 1020.210(b)(i); *Bank Secrecy Act (BSA)*, *supra* note 172.

202. Large currency transactions, regulated by 31 C.F.R. §§ 1010.310-315, are not discussed in this article given their limited relevance to P2P payments fraud.

i. Suspicious transaction reporting

After the financial institution has set up an account and completed a customer risk profile, it is supposed to be on the lookout for any activity in the account that is suspicious or out of the ordinary for the account. If the bank detects "any suspicious activity relevant to a possible violation of law or regulation," it must be reported if:

- it is conducted or attempted by, at, or through the bank,
- it involves or aggregates at least $5,000 in funds or other assets, and
- "the bank knows, suspects, or has reason to suspect that:
  - (i) The transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of funds or assets) as part of a plan to violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation;
  - (ii) The transaction is designed to evade any requirements of this chapter or of any other regulations promulgated under the Bank Secrecy Act; or
  - (iii) The transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction."[203]

A bank is also permitted to report other suspicious activity "it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by this section."[204] Finally, in addition to the above requirements, imposed on all "financial institutions" under the Bank Secrecy Act,[205] all banks are required to file a "Suspicious Activity Report" ("SAR") for insider abuse involving any amount, violations aggregating $5,000 or more where a suspect can be identified, and

203. 31 C.F.R. § 1020.320(a).

204. 31 C.F.R. § 1020.320(a)(1).

205. 31 U.S.C. § 5312(a)(2) (including in the definition of "financial institution" a long list that includes broker/dealers, casinos, and others).

violations aggregating $25,000 or more regardless of whether a suspect can be identified.[206]

Most banks have an automated system that looks for anomalous account activity which, if detected, will generate a suspicious activity alert.[207] Once suspicious activity is detected, a human gets involved, investigating the matter and deciding whether the bank should report the suspicious activity.[208] Banks tend to err on the side of over-reporting.[209]

Banks report suspicious activity by filing a SAR with FinCEN, which then refers the report to law enforcement, intelligence agencies, or entity supervisors (such as the Office of the Comptroller of the Currency for national banks).[210] SARS must be filed "no later than 30 calendar days after the date of initial detection by the bank of facts that may constitute a basis for filing a SAR."[211] Filing can be delayed up to sixty days after the bank detects the incident requiring a SAR if the bank does not have the identity of the suspect involved, in order to identify the suspect. [212] If the incident required "immediate attention," such as in the case of ongoing money laundering, the bank must also notify by telephone the appropriate law enforcement agencies.[213] If suspicious activity is ongoing, the bank is expected to file an updated SAR.[214] Banks must keep records supporting the SAR for five years from the date of filing the SAR, and those records must be made available to law enforcement and/or the bank's supervisors.[215] Reporters are immune from liability of any kind for filing a SAR.[216]

SARS are filed through an e-filing system. In order to file a SAR, the filer must register with FinCEN.[217] The SAR form itself is quite

206. *See generally* 12 C.F.R. § 21.11.

207. *The Truth About Suspicious Activity Reports*, BANK POL'Y INST. (Sept. 22, 2020), https://bpi.com/the-truth-about-suspicious-activity-reports/ [https://perma.cc/9BPQ-2N4X].

208. *Id.*

209. *Id.*

210. *Prepared remarks of Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network*, FINCEN (May 18, 2014), https://www.fincen.gov/news/speeches/prepared-remarks-jennifer-shasky-calvery-director-financial-crimes-enforcement-0 [https://perma.cc/FE4G-PMZ5]. FinCEN has been designated by the Secretary of the Treasury as the recipient of SARS pursuant to 31 U.S.C. § 5318(g)(4).

211. 31 C.F.R. § 1020.320(b)(3); *see also Bank Secrecy Act (BSA)*, *supra* note 172.

212. 31 C.F.R. § 1020.320(b)(3).

213. *Id.*

214. *Frequently Asked Questions Regarding the FinCEN Suspicious Activity Report (SAR)*, FINCEN, https://www.fincen.gov/frequently-asked-questions-regarding-fincen-suspicious-activity-report-sar [https://perma.cc/9J44-HG5F] (last visited Jan. 20, 2024).

215. 31 C.F.R. § 1020.320(d).

216. 31 U.S.C. § 5318(g)(3); 31 C.F.R. § 1020.320(f).

217. Registration is done at http://basefiling.fincen.treas.gov; *see The FinCEN Suspicious Activity Report Introduction & Filing Instructions*, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/sites

complicated, with ninety-eight data fields and a place for a narrative of the suspicious activity.[218] Field thirty-one of the SAR form asks the filer to categorize the type of fraud in one of eleven subcategories: ACH, business loan, check, consumer loan, credit/debit card, healthcare, mail, mass-marketing, pyramid scheme, wire, and other.[219]

ii. SAR Information Sharing

Once filed, there are strict rules about sharing the fact that a SAR has been filed or any of the information on the SAR. SAR filing is confidential, and no one–not anyone affiliated with the financial institution or the government–can disclose to persons involved in transactions reported that a report has been filed.[220] Sharing of SAR information is extraordinarily limited. Under Section 314(a) of the USA PATRIOT Act, FinCEN may share with financial institutions a list of persons suspected by law enforcement of terrorism or money laundering in order to find out if the financial institution is holding accounts for the suspect and regarding certain transactions by the suspect.[221] The request is instigated by law enforcement and carried out by FinCEN. In response, the financial institution must perform a search of its records and report the information requested.[222]

Under Section 314(b) of the USA PATRIOT Act, financial institutions and associations can register with FinCEN to be allowed to "transmit, receive, or otherwise share information with any other financial institution or association of financial institutions regarding individuals, entities, organizations, and countries for purposes of identifying and, where appropriate, reporting activities that the financial institution or association suspects may involve possible terrorist activity or money laundering."[223] Because of the definition of money laundering, this likely

---

/default/files/shared/TheNewFinCENSAR-RecordedPresentation.pdf [https://perma.cc/GVW3-P4PW] (FinCEN presentation explaining the e-filing system) (last visited Jan. 20, 2024).

218. See *FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Instructions*, FIN. CRIMES ENF'T NETWORK (Mar. 2015), https://bsaefiling.fincen.treas.gov/docs/FinCENSARElectronicFilingRequirements.pdf [https://perma.cc/B4QG-Z9WJ] for instructions on how to file a SAR, including a description of each of the data fields; *see also Frequently Asked Questions Regarding the FinCEN Suspicious Activity Report (SAR)*, *supra* note 214.

219. *FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Instructions*, *supra* note 218, at 97.

220. 31 U.S.C. § 5318(g)(2); 31 C.F.R. § 1020.320(e).

221. Pub. L. No. 107-56, §314(a), 115 Stat. 272 (2001) (codified as a note to 31 U.S.C. § 5311); 31 C.F.R. § 1010.520.

222. 31 C.F.R. § 1010.520(b)(3).

223. Pub. L. No. 107-56, §314(b), 115 Stat. 272 (2001) (codified as a note to 31 U.S.C. § 5311); 31 C.F.R. 1010.540. *See Section 314(b) Fact Sheet*, FIN. CRIMES ENF'T NETWORK (Dec. 2020), https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf [https://perma.cc/59VV-JMB9].

includes information regarding fraud, although reaching such a conclusion requires tracing through several statutes.[224] In order to participate in information sharing, both institutions must notify FinCEN of their intent to share information, and the notice lasts for one year.[225] The information shared can only be used to identify and report money laundering or terrorist activities; determine whether to establish or maintain an account or engage in a transaction; or help the financial institution comply with its Bank Secrecy Act requirements.[226] Financial institutions that participate in this type of information sharing must take care to guard the security and confidentiality of the information.[227] FinCEN has emphasized the importance of information sharing to identifying, reporting, and preventing financial crimes, and has "strongly" encourages financial institutions to participate in the 314(b) information sharing process, but there is no requirement to participate.[228]

Finally, pursuant to a new pilot program under the Anti-Money Laundering Act of 2020, financial institutions will be allowed to share information with their foreign branches and affiliates except for those in China, Russia, a jurisdiction that is a state sponsor of terrorism, a jurisdiction that is subject to sanctions imposed by the U.S. Government, and any jurisdiction that the Secretary of the Treasury has "determined cannot reasonably protect the security and confidentiality of such information."[229] On January 22, 2022, FinCEN issued a Notice of Proposed Rulemaking under this new statutory provision.[230] No final rule has been issued as of the publication of this Article.

---

224. 31 C.F.R. § 1010.505 (Money Laundering means an activity criminalized by 18 U.S.C. § 1956 or § 1957, or an activity that would be criminalized by 18 U.S.C. § 1956 or§ 1957 if it occurred in the United States"; 18 U.S.C. § 1956(c)(7); 18 U.S.C. § 1961(1).

225. 31 C.F.R. § 1010.540(b).

226. *Id.* § 1010.540(b)(4)(i).

227. *Id.* § 1010.540(b)(4)(ii).

228. *FinCEN Director Emphasizes Importance of Information Sharing Among Financial Institutions*, FIN. CRIMES ENF'T NETWORK (Dec. 10, 2020), https://www.fincen.gov/news/news-releases/fincen-director-emphasizes-importance-information-sharing-among-financial [https://perma.cc/8SU7-ELDL].

229. Anti-Money Laundering Act of 2020, Pub. L. 116-283, § 6212, 134 Stat. 4547, 4576 (Jan. 1, 2021), codified at 31 U.S.C. §5318(g)(8).

230. Fin. Crimes Enforcement Network, Notice of Proposed Rulemaking, 87 Fed. Reg. 3719 (Jan. 25, 2022); *see* Brendan Pedersen, *Banks Back Plan to Share SARS With Foreign Units. For Now.*, AM. BANKER (Jan. 24, 2022), https://www.americanbanker.com/news/banks-back-plan-to-share-sars-with-foreign-units-for-now [https://perma.cc/B7QX-F2RL].

c. *Third Party Payment Processors*

All of the above requirements relate to accounts opened directly by a customer. In an effort to evade the scrutiny described above, some bad actors, including fraudsters, might seek to deal with a third-party payment processor. In this instance, it is the third party payment processor who deals directly with the bank or financial institution.[231] However, the financial institution dealing with the third party payment processor has due diligence obligations in relation to the payment processor's clients, including looking for changes in the processor's business that change its risk profile, periodically reviewing and updating the processor's risk profile, having bank/processor contracts that allow the bank access to the processor's information, and periodically reviewing the processor's efforts to verify the processor's clients and business practices.[232] For this reason, dealing with third party payment processors can be cumbersome and risky for financial institutions, since they must know not just their own customer, but also their customer's customers.[233] As this Article goes to print, the Federal Reserve Board, FDIC, and OCC are considering a Proposed Interagency Guidance on Third-Party Relationships: Risk Management.[234]

d. *Money Mules*

Another way for bad actors, including fraudsters, to escape BSA/AML scrutiny while taking advantage of the U.S. banking system is to use

231. See Press Release, Dep't Just., Four Executives of Canadian Payment Processor Charge with Fraud and Money Laundering (June 20, 2019), https://www.justice.gov/opa/pr/four-executives-canadian-payment-processor-charged-fraud-and-money-laundering [https://perma.cc/F7WH-J58D], for a case example of a third-party payment processor being used to commit consumer fraud.

232. U.S. DEP'T TREASURY, NATIONAL MONEY LAUNDERING RISK ASSESSMENT 67 (2022), https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf [https://perma.cc/RHW3-2NFE]; *FFIEC Manual: Risk Associated with Money Laundering and Terrorist Financing, Trust and Asset Management Overview*, FED. FIN. INSTS. EXAMINATION COUNCIL, https://bsaaml.ffiec.gov/manual/RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/21 [https://perma.cc/TVU7-BTQD] (last visited Jan. 20, 2024); *Guidance on Payment Processor Relationships*, FED. DEPOSIT INS. CORP. (revised July 2014), https://www.fdic.gov/news/financial-institution-letters/2008/fil08127a.html [https://perma.cc/Y6XJ-JM9G].

233. *Guidance on Payment Processor Relationships*, *supra* note 232. Because of the risks associated with payment processors, FinCEN issued an advisory listing red flags that might indicate illicit activity by a third-party payment processor. *FIN-2012-A010: Risk Associated with Third-Party Payment Processors*, FIN. CRIMES ENF'T NETWORK (Oct. 22, 2012), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2012-a010 [https://perma.cc/9Y45-N5J6].

234. Proposed Interagency Guidance on Third-Party Relationships-Risk Management, 86 Fed. Reg. 38182 (July 19, 2021); Proposed Interagency Guidance on Third-Party Relationships-Risk Management, Extension of Comment Period to October 18, 2021, 86 Fed. Reg. 50789 (Sept. 10, 2021).

"money mules" to engage in transactions on the bad actor's behalf. Money mules help fraudsters evade detection by laundering funds through a third-party's account that may have been opened for a long period of time without arousing suspicion. A money mule is a person "who transfers or moves illegally acquired money on behalf of someone else."[235] The FBI divides money mules into three categories—those who are "unwitting" or "unknowing," those who are "witting," and those who are "complicit."[236] Unwitting or unknowing money mules are unaware that they are part of a larger scheme and likely were defrauded into participating in the scheme themselves, for example, through an online romance scheme or job offer.[237] Witting money mules willfully ignore red flags or act with willful blindness to the fact that they are engaged in fraudulent or illegal movement of money.[238] And, of course, complicit money mules know exactly what they are doing and participate fully in the scheme to defraud.[239]

Obviously, if the money mule is convinced to deal with a bank on behalf of a scammer, the financial institution may have significant difficulties executing its account-opening obligations. Although it might be possible to convince unwitting, unknowing, or witting individuals to give up the name of the beneficiary or true controller of the account, this is unlikely in the case of complicit money mules. However, even when a money mule is used, the bank should still be able to comply with its account monitoring and reporting obligations, since the account will show evidence of the same sorts of account activity that indicate fraudulent use of the account. In any event, the bank is required to follow its BSA/AML obligations when banking a money mule, even if the identity of the mule is legitimate and the mule is not the core fraudster.

2. Suggested changes to the BSA/AML regime that would help detect and prevent payments fraud

The current BSA/AML system for detecting, reporting, and preventing illicit financial conduct has a lot to offer by way of preventing, and sometimes remedying, payments fraud. Under the current system, the

---

235. *Money Mules*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/money-mules [https://perma.cc/BRS5-SYCU] (last visited Jan. 20, 2024); *see also* FIN. CRIMES ENF'T NETWORK, *supra* note 21.

236. *Money Mules*, *supra* note 235.

237. *Id.*

238. *Id.*

239. *Id.* The "red flag" indicators of COVID-19 money mule schemes can be found at FIN. CRIMES ENF'T NETWORK, *supra* note 21, at 6.

customer risk profile, combined with account monitoring, can expose fraud and lead to reporting and law enforcement involvement. It is certainly true that improvements to the beneficial ownership regime will go a long way in detecting and preventing payments fraud, and also make it difficult for fraudsters to form business entities with different names, one after the other, all hocking the same scams. But there are many tweaks and improvements to the BSA/AML system that would augment our societal ability to prevent, detect, and remedy fraud committed through P2P payment systems. The next Section of this Article discusses some of the BSA/AML changes that could have a big impact on controlling P2P payments fraud.

a. *Increase information required and reviewed at account opening*

Right now, at account opening, banks are only required to obtain the account holder's name, date of birth (for individuals), address, and ID number, such as social security or taxpayer identification number.[240] Banks are also required to have risk-based procedures for verifying the identity of each customer "to the extent reasonable and practicable."[241] These requirements are woefully inadequate in today's world, especially given the ease with which identities can now be stolen or created out of whole cloth, and the widespread use of money mules to open accounts on behalf of fraudsters.

One area for improvement would be to increase the information required from a prospective banking customer for purposes of confirming a potential customer's identity[242] This heightened identity requirement should be applied even to traditionally "low risk" banking products, such as checking accounts, because checking accounts opened

240. 31 C.F.R. § 1020.220(a)(2)(i).

241. *Money Mules*, *supra* note 235; § 1020.220(a)(2).

242. *See, e.g.*, Comment by Naftali Harris, Sentilink, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0093 ((indicating that approximately 3% of financial applications attempt identity fraud, and of those 41% will have an address with a consistent history for at least two years); Comment by Debra Geister, Socure, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0070; Comment by PayPal, Inc., FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0126; *see also* Comment by ID.me, Inc., FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0125 (suggesting that the National Institute of Standards Federal Digital Identity Guidelines into the CIP program requirements for banks).

with phony identification or by a money mule can be easily used to commit all kinds of fraud.[243]

Armed with this more robust identity information, it should be possible, and even required, for financial institutions to check the identity information they have gathered to see if the account is being opened in the name of an individual who has recently been the victim of identity theft, or by a person found to have committed identity theft. This could be determined by requiring banks to check the credit report of account applicants, and by setting up a central registry of identity theft victims and perpetrators.

In some cases, consumers who have been the victim of identity theft will request a freeze to their credit report with the three major credit reporting agencies (Experian, Equifax, and TransUnion). In this case, if a bank checks an individual potential customer's credit report there is at least a hope that the bank will be able to detect that the person opening the account is not likely who they say they are. There are also currently three consumer reporting companies that focus on check and bank screening, which might aid in detecting identity theft.[244] The problem is that there is currently no requirement for banks to pull a credit report when opening an account, report data to any particular company, or run identity checks through any system before opening an account. Instead, current guidelines merely require that banks "include, as appropriate, steps to ensure the accuracy and veracity of application information."[245] The details are left to each financial institution as part of their risk management. Without required participation in these credit reporting systems (and sharing of information across companies), there are natural limitations to the effectiveness of these systems.

Even better than a disbursed credit reporting system, a central registry for reporting the names and other identifying information for

243. Comment by Naftali Harris, Sentilink, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0093 (focusing on unemployment insurance and Paycheck Protection Program funding fraud during the COVID-19 pandemic).

244. According to the CFPB, these are: ChexSystems; Early Warning Services; and Telecheck Services. CONSUMER FINANCIAL PROTECTION BUREAU, LIST OF CONSUMER REPORTING COMPANIES 26–29 (2023), https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-companies-list_2023.pdf [https://perma.cc/VDK2-D2LB]. There are 3 other companies that focus on verifying payment information for merchants. *Id.* at 26, 27; *see also* Chi Chi Wu, *Account Screening Consumer Reporting Agencies: A Banking Access Perspective*, NAT'L CONSUMER L. CTR. (2016), https://cfefund.org/wp-content/uploads/2016/08/Account-Screening-CRA-Agencies-Banking-Access-report.pdf [https://perma.cc/X7VC-CMKF].

245. Letter from Richard Spillenkothen, Director, Bd. of Governors of the Fed. Reserve, to the Officer in Charge of Supervision and Supervisory Staff at each Federal Reserve Bank and to each Domestic and Foreign Banking Organization Supervised by the Federal Reserve (Apr. 26, 2001), https://www.federalreserve.gov/boarddocs/srletters/2001/sr0111.htm [https://perma.cc/HEN2-AHKA].

identity theft victims and perpetrators could help financial institutions spot the red flags of identity theft. At this time, there is no such central registry. Instead, data about identity theft is compiled and reported on an annual basis by the FTC.[246] While these reports provide a detailed description of the types of identity theft in the market and their prevalence, they do not really assist financial institutions with avoiding doing the bidding of identity thieves. A central registry would allow financial institutions to check the identity information they have against a detailed list of identity theft victims and perpetrators. This would go a long way in preventing identity thieves from opening a bank account in the name of their victim. A central registry for known synthetic identities would serve a similar function.[247]

These changes would make it easier for banks to detect fraudsters at account opening, allowing the bank to refuse to open an account for the fraudster and also diminishing the bank's account monitoring burden. Fewer accounts opened by fraudsters means less account monitoring down the road.[248] Banks could also be required to collect information about the expected activity for which the account will be used, rather than having this folded into the CDD risk-based approach.[249] This information could assist with an accurate risk profile against which to measure account activity and could help banks detect indicia of fraud and suspicious activity.

b. *Changes to the SAR form and content*

The current SAR reporting form is complex and relegates important information to the narrative section of the report. It also has eleven categories of fraud that are inadequate for describing some types of fraud and relegate a lot of reported fraudulent activity to the "other" category.[250]

246. For the most recent identity theft information report, see *Consumer Sentinel Network Data Book 2022*, FED. TRADE COMM'N (Feb. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf [https://perma.cc/C79R-EK67].

247. A synthetic identity combines a real person's information, such as their social security number, with falsified information to create a new identity. *What is Synthetic Identity Theft?*, EQUIFAX, https://www.equifax.com/personal/education/identity-theft/synthetic-identity-theft/ [https://perma.cc/YGS9-KXRY] (last visited Jan. 20, 2024).

248. *See* Comment by Debra Geister, Socure, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0070 (available at regulations.gov).

249. *See, e.g.*, Comment by Alan Ketley, The Wolfsberg Group, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0082 (available at regulations.gov).

250. The current categories are ACH, business loan, check, consumer loan, credit/debit card, healthcare, mail, mass-marketing, pyramid scheme, wire, and other. *FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Instructions*, *supra* note 218, at 97.

While other questions probe a bit deeper,[251] a more detailed description of the fraud committed is relegated to the narrative section.[252] It is currently possible for the public to search for the number of reports filed in a designated category.[253] This gives consumer advocates, banking industry representatives, and others the ability to at least see what is being reported and the level at which certain fraud is being reported. But SARs themselves, including the narrative field, are not publicly available. This means trends and nefarious activity described in the narrative section of the SAR are not detectable to anyone but FinCEN. Within FinCEN, searching successfully through the narrative section for trends would require word searching through the enormous volume of SARs filed each year,[254] and the success of this search might turn on whether those filing SARs used identical language to describe identical activity.

The complexities and confusion of reporting fraud can be seen in the FinCEN advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID 19).[255] In that advisory, FinCEN had to provide instructions for flagging an imposter scam or money mule scheme on the SAR form—and the instructions are neither obvious nor easy to use:

> SAR reporting, in conjunction with effective implementation of due diligence requirements by financial institutions, is crucial to identifying and stopping financial crimes, including those related to the COVID-19 pandemic. Financial institutions should provide all pertinent and available information in the SAR and narrative. Adherence to the filing instructions below will improve FinCEN's and law enforcement's abilities to effectively identify actionable SARs using the FinCEN Query system and pull information to support COVID-19- related investigations.
>
> - FinCEN requests that financial institutions reference this advisory by including the key term "COVID19 MM FIN-2020-A003" in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection

---

251. *See, e.g.*, *id.* (1) Field 35, called other suspicious activities, which allows for designation of "elder financial exploitation," "identity theft," and other subcategories, and (2) Field 39, which has a list of products involved in the suspicious activity, such as a debit or credit card.

252. *FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Instructions*, *supra* note 218.

253. FinCEN maintains a database in which one can search by institution type and category. *Suspicious Activity Report Statistics (SAR Stats)*, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/reports/sar-stats [https://perma.cc/SQQ4-2BBV] (last visited Jan. 20, 2024).

254. In 2022 alone FinCEN received just under 1.4 million reports for fraud just looking at depository institutions. *Id.*

255. FIN. CRIMES ENF'T NETWORK, *supra* note 21.

> between the suspicious activity being reported and the activities highlighted in this advisory.
>
> - Financial institutions should also select SAR field 34(z) (Fraud - other) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and COVID-19. Financial institutions should include the type of fraud and/or name of the scam or product (e.g., imposter scam or money mule scheme) in SAR field 34(z). In addition, FinCEN encourages financial institutions to report certain types of imposter scams and money mule schemes using fields such as SAR field 34(l) (Fraud- Mass-marketing), or SAR field 38(d) (Other Suspicious Activities- Elder Financial Exploitation), as appropriate with the circumstances of the suspected activity.[256]

This Article suggests several improvements to the SAR form that would make reporting fraud easier and more accurate and would make the reports filed more useful.

First, the SAR should be updated regularly as technology changes[257] and as new ways of committing crime and new fraud typologies emerge.[258] This would allow for more accurate reporting and avoid overuse of the non-specific "other" category when fraudulent activity is suspected.[259]

The SAR should contain fraud categories that are more "granular" so that a more detailed categorization of fraud is possible.[260] FinCEN should consider changing the SAR to be in conformity with the Federal Reserve's "FraudClassifier Model" rather than categorizing fraud based on the type of payment system or transaction involved.[261] The optimal SAR would classify fraud by asking about the type of fraud based on the

256. *Id.*

257. Comment by PayPal, Inc., FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0126 (available at regulations.gov).

258. Anonymous Comment, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0041 (available at regulations.gov); Comment by Bank of China New York, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0066 (available at regulations.gov).

259. Comment by PayPal, Inc., FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0126 (available at regulations.gov).

260. Comment by Bank of China New York, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0066 (available at regulations.gov).

261. Press Release, Board of Governors of the Federal Reserve System, Federal Reserve announces FraudClassifier Model to help organizations classify fraud involving payments (June 18, 2020, 1:00 p.m.), https://www.federalreserve.gov/newsevents/pressreleases/other20200618a.htm [https://perma.cc/99H3-XD37]; *see, e.g.*, Comment by Debra Geister, Socure, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0070 (available at regulations.gov).

FraudClassifer Model, the type of transaction (consumer loan, mortgage, sale of goods, etc.), and the payment method (including a new field that is peer-to-peer payment specific).[262]

The SAR form should also require information about the account and bank to which fraudulent payments were transferred.[263] Receiving banks should be expeditiously furnished with this information so that they can act quickly to monitor and potentially cut off the fraud pipeline and be the subject of enforcement scrutiny if they continue to allow fraudulent payments to flow through their bank.

These changes would give a much truer picture of the type of fraud being reported and the accounts and institutions involved. To the extent these SARS were shared with other financial institutions (see below), they would give other financial institutions a better idea of what to look for in executing their own BSA/AML policies and requirements. In lieu of and until these changes, FinCEN should at least provide clear instructions about how to report new types of fraud not reflected on the current SAR, such as P2P fraud, so that reporting is consistent and easy. [264]

Another improvement would be to allow banks to file a partial SAR immediately, rather than waiting the full thirty days to file a complete SAR,[265] and allowing banks to rank the importance of a SAR by including a "priority" designation on the SAR form.[266] In this way, if a bank detects suspected terrorist activity or a large volume of fraudulent activity, the report can indicate the urgency and size of a reported matter. Immediate reports—coupled with the identity of the receiving institution and information sharing to that institution—might be crucial in the case of payments fraud. After all, a fraudster can run many payments through an account during the thirty-to-sixty-day reporting window and then move the account to another institution, thereby avoiding detection. FinCEN could also augment the value of SARS to law enforcement and, if shared, to other banks, by allowing reporters to upload relevant documentation when a SAR is filed. This could include driver's licenses,

---

262. Comment by Kaley Schafer, National Association of Federally-Insured Credit Unions, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0063 (available at regulations.gov); Anonymous Comment, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0010 (available at regulations.gov).

263. Comment by National Consumer Law Center, National Community Reinvestment Coalition, National Consumers League, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0131 (available at regulations.gov).

264. Comment by Kaley Schafer, National Association of Federally-Insured Credit Unions, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0063 (available at regulations.gov).

265. *See, e.g.*, Comment by Peraton, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0057 (available at regulations.gov).

266. *See, e.g., id.*

passports, transaction videos, photographs, and other material that would assist with identifying, monitoring, and reporting fraudsters.[267]

c. *Increased sharing of SARS information*

The first clarification FinCEN must make is that information about possible fraudulent account activity can be shared under Section 314(b) of the USA PATRIOT Act by financial institutions and associations who register with FinCEN. This clarification is required because fraud is not specifically included in the type of information that can be shared under 314(b). Rather, the statute specifically allows sharing related to "money laundering or terrorism."[268] Determining that information about fraud can be shared as well under this provision requires tracing through several statutes.[269] Adding fraud specifically to the list of information that can be shared under 314(b) would clear up any confusion over whether this vital information can be shared.

Next, historical information about past fraud committed by current and prospective bank customers is crucial. In the current system, a bank's source of information regarding a potential customer is limited to information provided by the customer, information on individuals obtained from a credit reporting agency,[270] and information obtained through the voluntary 314(b) information sharing process, which covers possible terrorist activity or money laundering.[271] Beyond this, there are no other sources for determining a customer's banking behavior at other institutions. There is also no centralized list of crooks, similar to the "Specially Designated Nationals and Block Persons List (SDN)", maintained by the Office of Foreign Asset Control (OFAC), who have used other banks to scam consumers, used or served as money mules, or

267. *See, e.g.*, *id.*

268. Pub. L. No. 107-56, §314(b), 115 Stat. 272 (2001) (codified as a note to 31 U.S.C. § 5311); 31 C.F.R. § 1010.540; *see Section 314(b) Fact Sheet*, *supra* note 223.

269. 31 C.F.R. § 1010.505 ("Money Laundering means an activity criminalized by 18 U.S.C. § 1956 or § 1957, or an activity that would be criminalized by 18 U.S.C. § 1956 or § 1957 if it occurred in the United States"; 18 U.S.C. § 1956(c)(7); 18 U.S.C. § 1961(1).

270. According to the CFPB, there are six consumer reporting companies that focus on Check and Bank Screening: Cartefy Payment Solutions, LLC; ChecSystems; CrossCheck, Inc., Early Warning Services; Global Payments Check Services, Inc.; and Telecheck Services. *List of Consumer Reporting Companies*, CONSUMER FIN. PROT. BUREAU, https://www.consumerfinance.gov/consumer-tools/credit-reports-and-scores/consumer-reporting-companies/companies-list/ [https://perma.cc/U89K-Y73Z] (last visited Jan. 20, 2024).

271. Pub. L. No. 107-56, §314(b), 115 Stat. 272 (2001) (codified as a note to 31 U.S.C. § 5311); 31 C.F.R. § 1010.540; *see Section 314(b) Fact Sheet*, *supra* note 223; *see infra* Section B(1)(a)(iv)(b)(ii).

evidenced account activity that are known indicia of fraud.[272] Similarly, there is no place where fraud allegations are tabulated.

Without easily accessible and accurate historical information about prospective customers, it is not until a bank has had its own suspicions raised by account activity or requests from FinCEN under 314(a) that the bank learns that it may have banked a fraudster or money mule working with and on behalf of a scam artist. Increasing the information available to banks about prospective clients would enhance financial institution's ability to protect themselves, the banking system, and society at large from payments fraudsters. For this reason, the SAR system should allow for and even require greater information sharing among banks and from the government and law enforcement to banks.

Information sharing is a crucial aspect of decision-making in the arena of financial services. Indeed, it is common for financial institutions and financial services providers to rely on information about past conduct for purposes of making decisions about access to services and products in the future. For example, decisions whether to grant credit in the United States are based largely on the credit reporting system, which monitors and records the credit history of every individual, assigns a risk score, and constantly updates that score as information changes.[273] This information regarding behavior is the primary, and sometimes the only, factor financial services providers use in deciding whether to grant credit to individuals in the present and future, what sorts of pricing or limits to impose, and when to restrict ongoing access to open-end credit accounts.[274] The SAR process has the potential to help serve as this sort of system for banks, both in terms of initial account opening and ongoing monitoring, but because of information-sharing limitations, the process cannot serve that purpose as robustly as it might.

The need for this historical account behavior information is even more crucial in the real-time payments space, where payments are instantaneous and irrevocable. This is because return rates, a key indicator that someone is using an account to commit fraud, are not available since there are no payment returns. Return rates are calculated based on how often a payee's payments are returned due to insufficient funds, incorrect account numbers, or successfully disputed payments. Normal

---

272. *Specially Designated Nationals and Block Persons List (SDN) Human Readable Lists*, *supra* note 175.

273. *Credit Reports and Credit Scores*, FED. RSRV. BD., https://www.federalreserve.gov/creditreports/pdf/credit_reports_scores_2.pdf [https://perma.cc/9GMP-PGY3] (last visited Jan. 20, 2024); *How Do Lenders Use Credit Scores*, EQUIFAX, https://www.equifax.com/personal/help/lenders-creditscores/ [https://perma.cc/5ZS8-WBH4] (last visited Jan. 20, 2024).

274. Credit reports are regulated by the Fair Credit Reporting Act, codified at 15 U.S.C. § 1681-1681x.

return rates are about 1.25%.[275] High return rates can indicate nefarious activity by the payee because it reflects payments stopped or successfully disputed by the paying party.[276] Of course, in the world of P2P payments, which are settled instantly and irrevocably, there are no returned payments. As a result, this very useful indicator of fraud is not available. (Zelle reports that it voluntarily notifies recipient banks when fraud is alleged.[277]) This only amplifies the need for more information at the time a financial institution is deciding whether to bank a customer, and on an ongoing basis for purposes of account monitoring. For all of these reasons, increased secure information-sharing will be a key component of preventing fraud through the BSA/AML modernization process. As put by one commentor in response to the FinCEN NPRM, "Data-sharing regarding fraud methodologies and perpetrators is one of the greatest means of early and preventive detection of fraud, money laundering, and other financial crimes."[278]

First, the government needs to share more information with banks so that they can carry out their BSA/AML obligations, and protect themselves, the banking system, and consumers from fraud. FinCEN regularly provides information about red flags and typologies for crime and money laundering.[279] In the area of elder fraud, FinCEN issued an Advisory on Elder Financial Exploitation, but the red flags in the advisory all dealt with detecting when a bank customer has been or is about to be the victim of fraud.[280] While this is helpful to a financial institution trying to protect its elderly customers, FinCEN also needs to provide advisories, red flags, and identifying information about those engaging in fraudulent conduct.[281] FinCEN also needs to develop a mechanism for

275. Reyes v. NetDeposit, LLC, 802 F.3d 469, 476 (3rd Cir. 2015).

276. *See, e.g.*, *id.* at 469 (evaluating whether class could be certified based on high return rates (25 times the national average of 1.25%) of telemarketing scheme that authorized debits from plaintiffs' accounts).

277. Zelle's page for reporting frauds says "While we are unable to assist with getting your money back, it is important to us that users have the ability to report this experience. We will report the information you provide to the recipient's bank or credit union to help prevent anyone else from having the same experience." Jon Healey, *Do You Use Zelle? Here's How To Spot Increasingly Common Scams*, LOS ANGELES TIMES (Oct. 7, 2022), https://www.latimes.com/business/technology/story/2022-10-07/zelle-banks-may-not-cover-the-losses-from-scams [https://perma.cc/X8X7-5BC9].

278. Comment by Fraud.net, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0134 (available at regulations.gov).

279. *See* Alerts/Advisories/Notices/Bulletins/Fact Sheets A catalog of current Alerts, Advisories, Notices, Bulletins, and Fact Sheets can be found at https://www.fincen.gov/resources/advisories-bulletinsfact-sheets.

280. *See, e.g.*, *FinCEN Advisory on Elder Financial Exploitation*, FIN. CRIMES ENF'T NETWORK (June 15, 2022), https://www.fincen.gov/news/news-releases/fincen-issues-advisory-elder-financial-exploitation [https://perma.cc/M4U9-ZNUV].

281. *See* Debra Geister, Comment Letter on FinCEN Request for Information on Ways to Streamline, Modernize, and Update the Anti-money Laundering and Countering the Financing of

notifying receiving banks when one of their customers has been identified as having committed fraud by a sending bank. This will give banks a view of the full field when deciding whether to open an account, whether to freeze a transaction or entire account, and whether to close an account. This, in turn, will help banks keep fraudsters from committing fraud through their accounts.

FinCEN also needs to provide information to banks indicating which SARS have been useful to law enforcement and why.[282] This sort of feedback would help a bank that has submitted a SAR make a decision as to whether the account holder poses a threat and whether the account should be closed.[283] It would also improve the quality of SAR filings. This would be a boost to the entire system, which relies on uniform, timely, and accurate reporting to detect and stop financial crime.[284]

Terrorism (AML/CFT) Regime of the United States (Feb. 11, 2022), https://www.regulations.gov/document/FINCEN-2021-0008-0001/comment ("This referential data set that includes not just the 'how' but also the 'who' would significantly impact the detection capabilities . . . . Secure data sharing mechanism that preserves privacy and security while assisting financial services in detecting cross-institutional behavior and velocities can also help create a stronger financial services system.")

282. *See, e.g.*, Dennis Schwartz, Comment Letter on FinCEN Request for Information on Ways to Streamline, Modernize, and Update the Anti-money Laundering and Countering the Financing of Terrorism (AML/CFT) Regime of the United States (Feb. 14, 2022); James Richards, Comment Letter on FinCEN Request for Information on Ways to Streamline, Modernize, and Update the Anti-money Laundering and Countering the Financing of Terrorism (AML/CFT) Regime of the United States (Feb. 11, 2022); Alison Clew, Comment Letter on FinCEN Request for Information on Ways to Streamline, Modernize, and Update the Anti-money Laundering and Countering the Financing of Terrorism (AML/CFT) Regime of the United States (Feb. 13, 2022); Kevin J. Lampeter, Comment Letter on FinCEN Request for Information on Ways to Streamline, Modernize, and Update the Anti-money Laundering and Countering the Financing of Terrorism (AML/CFT) Regime of the United States (Feb. 14, 2022); Elizabeth M. Sullivan, Comment Letter on FinCEN Request for Information on Ways to Streamline, Modernize, and Update the Anti-money Laundering and Countering the Financing of Terrorism (AML/CFT) Regime of the United States (Feb. 14, 2022); Alan Ketley, Comment Letter on FinCEN Request for Information on Ways to Streamline, Modernize, and Update the Anti-money Laundering and Countering the Financing of Terrorism (AML/CFT) Regime of the United States (Feb. 14, 2022); Kaley Schafer, Comment Letter on FinCEN Request for Information on Ways to Streamline, Modernize, and Update the Anti-money Laundering and Countering the Financing of Terrorism (AML/CFT) Regime of the United States (Feb. 11, 2022); Bank of China New York, Comment Letter on FinCEN Request for Information on Ways to Streamline, Modernize, and Update the Anti-money Laundering and Countering the Financing of Terrorism (AML/CFT) Regime of the United States (Feb. 11, 2022); Fraud.net, Comment Letter on FinCEN Request for Information on Ways to Streamline, Modernize, and Update the Anti-money Laundering and Countering the Financing of Terrorism (AML/CFT) Regime of the United States (Feb. 14, 2022); Geister, *supra* note 282. All sources cited in this footnote are available at: https://www.regulations.gov/document/FINCEN-2021-0008-0001/comment.

283. Comment by Michael Holland, FirstBank, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0092 (available at regulations.gov) (stating that banks would then be able to become more of a "partner in the fight against financial crimes.").

284. *See, e.g.*, Comment by Dennis Schwartz FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0048 (available at regulations.gov).

Second, banks need to be allowed, and in some cases required, to share more information with each other so that when making decisions about a prospective or current customer any given bank has a full picture of the customer. Information is crucial to these decisions, and any given bank is unlikely to have a full picture of a prospective or current account holder. This type of information sharing could be accomplished by making 314(b) information sharing participation mandatory for all financial institutions, or at least encouraging greater participation.[285] Receiving banks (the fraudster's bank) should be required to cooperate with investigations conducted by sending banks (the victim's bank). With information from the receiving bank, the sending bank would have the ability to file a SAR that is more complete and useful in regard to stopping the fraudster. Once information is shared, banks should also be allowed to jointly investigate and report suspicious activity. [286] And the type of information that can be shared under 314(b) should be expanded so that "banks can freely discuss other types of potentially criminal activity, such as elder financial exploitation, kiting, check fraud, etc."[287]

Finally, FinCEN could either maintain, or allow for private maintenance of, a list of individuals and entities that have committed payments fraud using their bank account, and of identities that have been stolen or are synthetic.[288] To make this list effective, FinCEN must make sure the list is centralized and that use by both providers and recipients of information is mandatory. This list could be similar to the "Specially

285. *See, e.g.*, Mechanics Bank, Comment Letter on FinCEN Request for Information on Ways to Streamline, Modernize, and Update the Anti-money Laundering and Countering the Financing of Terrorism (AML/CFT) Regime of the United States (Feb. 4, 2022); Richards, *supra* note 282; Clew, *supra* note 282; Ketley, *supra* note 282; FeatureSpace, Comment Letter on FinCEN Request for Information on Ways to Streamline, Modernize, and Update the Anti-money Laundering and Countering the Financing of Terrorism (AML/CFT) Regime of the United States (Feb. 14, 2022); Sullivan, *supra* note 283. All sources cited in this footnote are available at: https://www.regulations.gov/document/FINCEN-2021-0008-0001/comment.

286. Richards, *supra* note 283.

287. Anonymous, Comment Letter on Docket Number FINCEN-2021-0008 (Feb. 4, 2022), https://www.regulations.gov/comment/FINCEN-2021-0008-0041 ("With the increase in elder financial exploitation, for example, financial institutions can work together along with Adult Protective Services to help older adults. Rather than having to close the accounts of potential victims, only to have them go to other financial institutions and continue the cycle of abuse, a more open 314(b) program could prevent bigger losses to individuals and would hopefully stop the criminals from going after older adults.").

288. One payments company, Plaid, has introduced an anti-fraud network called Beacon which provides member financial institutions with a notification when someone who has been associated with fraud tries to open a new account. *Beacon*, PLAID, https://plaid.com/products/beacon/ [https://perma.cc/G6YH-T9GL] (last visited Feb. 18, 2024); Kate Fitzgerald, *Plaid leans on Banks, Fintechs to Create a Stolen-Identity Database.* AM. BANKER (June 22, 2023, 8:01 AM), https://www.americanbanker.com/payments/news/plaid-leans-on-banks-fintechs-to-create-a-stolen-identity-database [https://perma.cc/L4TZ-67UQ].

Designated Nationals and Blocked Persons List (SDN)", maintained by the Office of Foreign Asset Control (OFAC)[289] or could simply look like the ACH terminated originator list made available by the National Automated Clearing House Association (NACHA) to users of the ACH payments network.[290] The terminated originator list does not prohibit banks from banking those on the list, but it does help banks screen their potential and current customers and augments their ability to perform their customer due diligence and other "know your customer" functions.[291]

The Anti-Money Laundering Act of 2020 recognizes the utility of SARS information-sharing and requires the Secretary of the Treasury to "convene a supervisory team of relevant Federal Agencies, private sector experts in banking, national security, and law enforcement, and other stakeholders, to examine strategies to increase cooperation between the public and private sectors for purposes of countering illicit finance, including proliferation finance and sanctions evasion."[292] The above suggestions should be included in the strategies considered for expanded information sharing.

d. *Sharing of Beneficial Ownership information*

As indicated *infra*, the new Beneficial Ownership rule requires that information about beneficial ownership be shared with FinCEN.[293] The next crucial step is to create a central beneficial ownership registry and make that registry available through a secure portal to all financial institutions.[294] Making this information available to financial institutions

289. *Specially Designated Nationals and Block Persons List (SDN) Human Readable Lists*, *supra* note 175.

290. *Risk Management Portal*, NACHA, https://www.nacha.org/nacha-risk-management-portal [https://perma.cc/2XB9-EY9N]; *see* Letter from Nat'l Consumer L. Ctr., Nat'l Cmty. Reinvestment Coalition & Nat'l Consumers League, Comment Letter on Request for Information Regarding Review of Bank Secrecy Act Regulations and Guidance (Docket Number FinCEN-2021-0008-0131) (Feb. 14, 2022), https://www.regulations.gov/comment/FINCEN-2021-0008-0131.

291. *See Risk Management Portal*, *supra* note 290.

292. Pub. L. No. 116-283, § 6214, 134 Stat. 4547, 4579 (Jan. 1, 2021).

293. Corporate Transparency Act, Pub. L. 166-283, Title LXIV, 134 Stat. 4604, 4610–12 (Jan. 1, 2021); Fin. Crimes Enforcement Network et al., Beneficial Ownership Information Reporting Requirements Final Rule, 87 Fed. Reg. 59498 (Sept. 30, 2022); 31 C.F.R. § 1010.380.

294. Comment by Mechanics Bank, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0010 (available at regulations.gov); Comment by Debra Geister, Socure, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0070 (available at regulations.gov); Comment by Michael Holland, FirstBank, 2, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0092 (available at regulations.gov); Comment by PayPal, Inc., FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0126 (available at regulations.gov); Comment by Fraud.net, FINCEN Docket Number FINCEN-2021-0008, Comment ID FINCEN-2021-0008-0134 (available at regulations.gov).

would allow financial institutions to better perform their identification requirements and detect anomalies when new accounts are opened. Any indication that the beneficial owners do not match the entity identification would be a red flag that could prompt the bank to deny access to an account, lead to reporting to FinCEN, and help both law enforcement and financial institutions prohibit access to the financial system by those who want to hide behind a real or shell business entity.

IV. CONCLUSION

Protecting consumers from P2P manipulation payments fraud is essential in today's complex and fast-moving P2P payments world. To accomplish this, Congress and the CFPB must clarify and change the law so that victims of these scams have a right to have their bank accounts recredited. Correlative changes must also be made to leave the loss for fraud with the fraudsters, if they can be found, and with the receiving banks who bank them, if the fraudster cannot be found. A robust P2P system that is safe and effective for everyone requires a combination of detection, prevention, and remedy, and will incentivize financial institutions to protect consumers and the financial system from those who would use it for fraudulent gain.

V. EPILOGUE – UPDATES FROM 2023 AND THE FIRST QUARTER OF 2024

Since this article was completed in early 2023, fraud on Zelle and other P2P payments platforms has continued to harm consumers.[295] In the first

295. *See, e.g.*, Michael Finney & Renee Koury, *Bank of America Imposters Renew Zelle Scam, Telling Victims 'Ignore Fraud Warning'*, ABC 7 NEWS (Aug. 5, 2023), https://abc7news.com/bank-of-america-zelle-scam-fraud-warning/13599954/ [https://perma.cc/PBZ4-HM7X]; Shannon Behnken, *Despite Zelle Policy Change, Bank Denies Tampa Woman's Fraud Claim*, NEWSCHANNEL 8 (Nov. 20, 2023, 6:08 PM), https://www.wfla.com/8-on-your-side/better-call-behnken/despite-zelle-policy-change-bank-denies-tampa-womans-fraud-claim/ [https://perma.cc/V8MB-RDM8]; Larissa Bungo, *Scammers Impersonate Well-Known Companies, Recruit for Fake Jobs on LinkedIn and Other Job Platforms*, FED. TRADE COMM'N, CONSUMER ADVICE (Aug. 8, 2023), https://consumer.ftc.gov/consumer-alerts/2023/08/scammers-impersonate-well-known-companies-recruit-fake-jobs-linkedin-and-other-job-platforms [https://perma.cc/NK22-YKD2]; Amy Hebert, *Do You Use Payment Apps like Venmo, CashApp, or Zelle? Read This*, FED. TRADE COMM'N CONSUMER ALERT (Aug. 14, 2023), https://consumer.ftc.gov/consumer-alerts/2023/08/do-you-use-payment-apps-venmo-cashapp-or-zelle-read [https://perma.cc/M8FH-S7FX]; JILENNE GUNTHER, FIGHTING FINANCIAL EXPLOITATION ON PERSON-TO-PERSON PAYMENT PLATFORMS: WHAT CONSUMERS WANT (AARP Public Policy Institute 2024), https://www.aarp.org/content/dam/aarp/ppi/topics/work-finances-retirement/fraud-consumer-protection/banksafe-p2p-exploitation.doi.10.26419-2Fppi.00213.001.pdf [https://perma.cc/H2MU-FY5C]. The CFPB issued a report addressing the particular harm these scams can cause for servicemembers. CONSUMER FIN. PROT. BUREAU, OFF. SERVICEMEMBER AFFS. ANNUAL REPORT,

three quarters of 2023 alone, the Federal Trade Commission received 48,835 complaints of fraud involving a payment app or service with a reported loss to consumers of $151.9 million.[296] The number of scams like those discussed in this article are forecast to continue growing exponentially.[297]

In response to this growing problem and calls for industry and regulatory solutions, several things have taken place. On the industry side, in response to pressure from regulators, Zelle adopted a policy of refunding customers who fall victim to an imposter scam.[298] While this policy is certainly a step in the right direction, it addresses only one type of manipulation payments fraud, and its effectiveness and ease of use remain to be seen. For now, refund decisions are made on a case-by-case basis and require a phone call to Zelle for anyone not using Zelle through their financial institution.[299] Right now, Zelle is the only company that has instituted a voluntary refund program, although Senators have urged others to take similar steps.[300]

As of this article's publication, neither the House of Representatives nor the Senate have introduced a bill to address the problems discussed in this article. However, the Senate Committee on Banking, Housing, and Urban Affairs did hold a hearing on Thursday, February 1, 2024, entitled "Examining Scams and Fraud in the Banking System

---

JANUARY – DECEMBER 2022 (2023), https://files.consumerfinance.gov/f/documents/cfpb_osa-annual-report_2022.pdf [https://perma.cc/U769-KKUQ].

296. *Fraud Reports by Federal Trade Commission*, TABLEAU PUBLIC (Feb. 8, 2024), https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods [https://perma.cc/C7JQ-4ZD6].

297. One recent study predicted a 50% rise in these scams by 2027. Tatiana Walk-Morris, *Authorized Payments Scams Climb in the U.S.*, PAYMENTS DIVE (Dec. 14, 2023), https://www.paymentsdive.com/news/authorized-push-payment-fraud-banks-financial-services-ACI/702493/ [https://perma.cc/AF8H-SPWM]. The United States is not the only country dealing with this problem.

298. *Frequently Asked Questions: I Believe I've Been a Victim of an Imposter Scam. Who Should I Contact?*, ZELLE, https://www.zellepay.com/faq/i-believe-ive-been-victim-imposter-scam-who-should-i-contact [https://perma.cc/Y7UK-5CXQ] (last visited Feb. 3, 2024); Anna Hrushka, *Banks Too Slow to Address P2P Payment Scams, CFPB's Chopra Says*, BANKING DIVE (June 14, 2023), https://www.paymentsdive.com/news/banks-slow-p2p-payment-scams-chopra-zelle-cfpb-senate-menendez/652875/ [https://perma.cc/TU4M-JS8W]; Hannah Lang, *Payments App Zelle Begins Refunds for Imposter Scams After Washington Pressure*, REUTERS (Nov. 13, 2023, 1:05 PM), https://www.reuters.com/technology/cybersecurity/payments-app-zelle-begins-refunds-imposter-scams-after-washington-pressure-2023-11-13/ [https://perma.cc/NTT5-YFUA].

299. *See, e.g.*, Natalie Campsis, *Scammed Out of Money on Zelle? You Might Be Able to Get it Back*, FORBES ADVISOR (Nov. 14, 2023, 8:23 PM), https://www.forbes.com/advisor/money-transfer/zelle-users-refunded-after-scams/ [https://perma.cc/3CXG-JFNZ].

300. Press Release, Sherrod Brown, Chairman S. Banking, Hous., & Urban Affs. Comm., U.S. Senate, Brown, Colleagues Urge PayPal to Protect Venmo Users from Fraud (June 15, 2023), https://www.brown.senate.gov/newsroom/press/release/sherrod-brown-colleagues-urge-paypal-protect-venmo-users-from-fraud [https://perma.cc/W4M6-UVLE].

and Their Impact on Consumers,"[301] at which consumer organizations urged Congress to take action to protect consumers who use P2P apps.[302] Whether this will lead to legislation also remains to be seen.

On the regulatory side of the problem, in November 2023 the CFPB issued a Notice of Proposed Rulemaking proposing a rule to bring larger consumer payments market participants under the CFPB's supervisory authority.[303] The rule, if adopted, would cover non-bank entities that provide "general use digital consumer payment applications with an annual volume of at least five million consumer payment transactions" and that are not a small business concern.[304] While the rule would not create new consumer protections in the P2P payments space,[305] it would bring covered market participants "within the CFPB's supervisory jurisdiction."[306] The comment period for the proposed rule closed on January 8, 2024.[307] On March 1, 2024, the FTC announced a final rule that prohibits the impersonation of government, businesses, and their officials or agents in interstate commerce.[308] This rule should help the FTC pursue and seek damages from scam artists who use spoofing to steal money from consumers. It will also provide the FTC with funds from which to compensate victims.

Not surprisingly, manipulation fraud is a problem around the world.[309] One report based on consumer polling found that "a fifth of consumers worldwide have been victims of payment fraud in the past four years" (ending in 2023) and that a quarter of that group had been the victim of manipulation fraud (called Push Payment fraud in some

---

301. The hearing can be watched on the Committee Website. *Examining Scams and Fraud in the Banking System and Their Impact on Consumers Before the S. Comm. On Banking, Hous., & Urban Affs.*, 118th Cong. (Feb. 1, 2024), https://www.banking.senate.gov/hearings/examining-scams-and-fraud-in-the-banking-system-and-their-impact-on-consumers [https://perma.cc/D67V-HDVX]. The comments of the three witnesses, as well as Member Statements from Chairman Sherrod Brown (D–Ohio) and Ranking Member Tim Scott (R – South Carolina), can also be downloaded. *Id.*

302. *Examining Scams and Fraud in the Banking System and Their Impact on Consumers Before the S. Comm. On Banking, Hous., & Urban Affs*, 118th Cong. (2024) (statement of Carla Sanchez-Adams, National Consumer Law Center) [hereinafter *Statement of Carla Sanchez-Adams*].

303. Defining Larger Participants of a Market for General-Use Digital Consumer Payment Applications, 88 Fed. Reg. 80197 (proposed Nov. 17, 2023) (to be codified at 12 C.F.R. 1090.109).

304. *Id.* at 80199.

305. *Id.* at 80198.

306. *Id.* at 80201.

307. *Id.* at 80197.

308. Trade Regulation Rule on Impersonation of Government and Businesses, 89 Fed. Reg. 15017 (Mar. 1, 2024) codified at 16 C.F.R. part 461.

309. *See, e.g.*, WORLD BANK GRP., FRAUD RISKS IN FAST PAYMENTS (Oct. 2023), https://fastpayments.worldbank.org/sites/default/files/2023-10/Fraud%20in%20Fast%20Payments_Final.pdf [https://perma.cc/Y2DH-DGG4].

countries).[310] Although this Article focuses on the problem and solutions in the U.S., legislators and regulators in the U.S. should take note of the approach to this problem taken by other countries. In particular, the United Kingdom's Payment Systems Regulator announced a new rule in December 2023 requiring Britain's banks to reimburse customers who fall victim to manipulation fraud, with the reimbursement limited to a maximum of 415,000 pounds.[311]

Finally, courts in the U.S. have begun to address manipulation fraud in different types of civil lawsuits. In one class action lawsuit, a District Court Judge in California ruled that Bank of America customers who were defrauded using Zelle through their bank account could pursue a claim for breach of contract against the bank.[312] In the slip opinion denying the bank's motion to dismiss, the judge held that the word "unauthorized" in the contract between Bank of America and its depositors, which stated that Zelle users "will have no liability for unauthorized transactions" if they met notification requirements, was an ambiguous term. The court further held that the term was "susceptible to two reasonable interpretations: Defendant's version, which construes an unauthorized transaction as one initiated by a third party without an accountholder's consent; and Plaintiff's version, which construes an unauthorized transaction as any transaction involving fraud."[313] The contract's meaning will now be determined by the trier of fact.

In another suit, Wells Fargo was accused of aiding and abetting a Ponzi scheme when it ignored its own anti-money laundering policies and allowed the perpetrators to maintain and use their Wells Fargo accounts to receive payments from their victims through Zelle and Venmo.[314] The suit settled in March 2023 for $26.6 million.[315] In another suit, investors filed a derivative shareholder lawsuit in May 2023 against

---

310. Tatiana Walk-Morris, *Fraud Losses to Surpass $40B by 2027: Report*, PAYMENTS DIVE (June 16, 2023), https://www.paymentsdive.com/news/fraud-losses-realtime-payments-banks-aci-push-payment-scams/653219/ [https://perma.cc/8ZCE-S7GG].

311. Huw Jones, *UK Banks Face 'Step Change' Rule to Reimburse Defrauded Customers*, REUTERS (Dec. 19, 2023, 11:16 AM), https://www.reuters.com/business/finance/uk-banks-face-step-change-rule-reimburse-defrauded-customers-2023-12-19/ [https://perma.cc/AV6G-GK9R]; *Statement of Carla Sanchez-Adams*, *supra* note 303, at 12; *UK App Fraud Rules Will Keep Faster Payments Safer Long Term, Experts Say*, PYMNTS (May 2, 2023), https://www.pymnts.com/news/security-and-risk/2023/uk-app-fraud-rules-will-keep-faster-payments-safer-long-term-experts-say/ [https://perma.cc/ED43-L3D9].

312. Tristan v. Bank of Am., 2023 WL 4417271, at *12–13 (D. Ct. Ca. June 28, 2023).

313. *Id.*

314. Jessica Corso, *Wells Fargo to Settle Ponzi Suit Claims for $26.6M*, LAW360 (Mar. 21, 2023, 8:06 PM), https://www.law360.com/articles/1588293/wells-fargo-to-settle-ponzi-suit-claims-for-26-6m [https://perma.cc/YQ9Y-2ECD].

315. *Id.*

JPMorgan, claiming JP Morgan "breached its fiduciary duty and jeopardized the bank's reputation by not reimbursing customers for fraudulent transfers made on payments platform Zelle."[316] JPMorgan filed a motion to dismiss the lawsuit on August 1, 2023, which was still pending at the time this article went to print.[317]

Reigning in abuses on P2P payment platforms is crucial to everyone in the faster payments market, including regulators, financial institutions, and consumers. There are new developments in this area almost every week, including tech solutions that can help with catching fraudsters. Clearly, there will be more to come.

316. Henrik Nilsson, *JPMorgan Leaders Sued for Inaction on Booming Zelle Fraud*, LAW360 (May 18, 2023, 5:18 PM), https://www.law360.com/articles/1678959/jpmorgan-leaders-sued-for-inaction-on-booming-zelle-fraud [https://perma.cc/UG4P-WKXH]; *see* IMG Holding LLC, v. Dimon, 2023 WL 3582369 (Del.Ch.).

317. Jennifer Kay, *Dimon, JPMorgan Deny Board Failed in Zelle Fraud Claims Response*, BLOOMBERG LAW (Jan. 31, 2024, 12:42 PM), https://news.bloomberglaw.com/banking-law/dimon-jpmorgan-deny-board-failed-in-zelle-fraud-claims-response [https://perma.cc/6EVX-M3BT].