Informed Consent: A Potential Solution for Approved Push Payment (APP) Fraud

Problem Statement – Individuals and companies that are willfully defrauding customers are using faster payment options like Zelle, RTP and FedNow to receive payments, which are irrevocable. Defrauded customers have no recourse, unlike card and ACH payment options. In the interest of protecting consumers, there is discussion of making the Financial Institutions (FIs) liable for any fraud their customers may encounter using faster payment options. If enacted, the result would be FIs being liable when their customer used a faster payment type as it was intended, but the resulting transaction results in "fraud." In fact, there would be no arbiter of whether fraud existed; it would simply be the customer claiming fraud that would trigger the institution's liability. If financial institutions have the burden of liability, it could result in restricting customer access to faster payment options. Sending banks need the ability to provide their customers information about known suspect receivers before they initiate a push credit.

Background – The specific fraud that is the target of this document is Approved Push Payment (APP) fraud. It is "Approved" as the FI's customer initiates the transaction and uses the FI's provided online or mobile app user interface to provide the instructions on the amount and receiver of the credit. It is a "Push Payment" since the customer is authorizing a credit to be delivered in real time to a 3rd party individual or company. Their FI gives their customer an "Are You Sure?" type of message, and once the customer clicks to send the credit, the FI debits the account and provides an irrevocable credit to the designated receiver. If the sender does not receive the goods or services they believe they are contracting for, there is no option for that customer to initiate a return. They can ask their FI to request a return, but there is no obligation for the receiving FI to honor that request. It is inherent that the sender of an irrevocable faster payment, such as Zelle, RTP or FedNow have full knowledge and understanding of who they are paying and agree that there is no recourse for reversing the transaction. Financial institutions provide instructions as a part of the user experience to alert the customer that the credit pushed is irrevocable and also provide educational documents and videos to advocate for the safe usage of faster payment options.

Beginning in 2022, a series of stories began to appear in major news publications and broadcasts highlighting the "rampant Zelle fraud problem …" These stories all center on the fact that fraudsters are using the irrevocability of Zelle as the reason to use it for their payments. What the stories all omit is that in all but a few cases, the defrauded customers all willingly sent the money to the fraudsters, using Zelle exactly as it was intended. The fraud isn't a Zelle problem. Fraudsters have been around since time immemorial. The fact that there is now a faster payment option called Zelle, and fraudsters request being paid that way does not make Zelle any more prone to fraud than any other payment mechanism. This story

7813 Office Park Blvd, Baton Rouge, LA 70809
(225) 924-8015

(https://www.wfla.com/8-on-your-side/better-call-behnken/zelle-fraud-cases-explode-customers-lose-millions/) from early 2023 seems to imply that "Zelle" fraud is being committed by stealing credentials of authorized users. While possible, there is no evidence that any significant cases of unauthorized access of online banking is the source of the fraud being reported.

Existing Fraud Prevention Measures Inadequate for APP Fraud – As long as there have been payments, there has been payment fraud. The elements of Reg E are specifically targeted to provide consumers relief in the situation where an unauthorized debit is pushed to their transaction account or similarly when an unauthorized charge is pushed to their credit card account. In both these examples, there is a process for the customer to signify that they did not authorize the charges and the financial institution reimburses the customer and chases the bad actor for the recompense. This likely means an ACH return or card chargeback using the rules of those systems to reimburse the financial institution. Fraud mitigation was centered on keeping unauthorized entities from having access to account holder private information such as account and routing numbers, as well as identifying and remediating malware and the resulting account takeover or similar cybercrime activities. Entities such as Nacha compiled databases of known bad originators, and Originating FIs were held accountable to limit the number of unauthorized returns that were received.

APP fraud is distinctly different in that there is zero fraud as a part of the payment itself. The customer knowingly uses a faster payment option to complete a transaction, but the receiver turns out to be fraudulent (or just inept). Maybe the customer didn't really understand what they were buying. Maybe there was an error in what the buyer and seller thought was being exchanged. Maybe the seller is an outright fraudulent person or entity. Regardless of why, the fact that a customer pushed a credit using faster payments is not an element of the fraud. It worked exactly as it was intended. Consider this example, an individual in Florida contracts to buy a dog from a breeder in Virginia. The breeder asks for $1,000.00 to be sent via Zelle (the example is identical if you substitute RTP or FedNow). The buyer complies and uses the bank's mobile app to complete the push credit of $1,000.00. Then, the customer gets no dog. Or gets an ill dog. Or gets a different dog. Or gets a cat. They contact the company to attempt to remediate the matter, and the company says, too bad, you got what you got. Regardless of "why" the customer is dissatisfied, the faster payment in this example played no part of the fraud. If the transaction had been settled with cash, or a check or a wire or via ACH, the fraud would have been exactly the same. The only difference is that the faster payment option has no recourse, no ability for the dissatisfied customer to reverse their push credit. Yet that is not a flaw in the faster payment system, it is a feature and the customer was given multiple fair warnings about the finality of their payment.

None of the existing fraud mechanisms can alert a customer about a potential bad receiver. The receiving FI may know that there are complaints about a receiver or has received return requests on a receiver. The originating FI may have reported that their customer has claimed that a receiver is fraudulent (in fact both The Clearing House and the Federal Reserve require FIs to report suspect bad receivers). However, none of those reported incidents of suspected fraud are available to the one entity that desperately needs it; that is the consumer who is

about to send a push credit. What good is reporting suspect bad receivers if the information is not available to senders BEFORE they push a credit?

Why Can't Customers Have Information Like Amazon or eBay Provides? – When you shop online at companies like Amazon and eBay, a buyer is provided with a wealth of information about the product they are purchasing. More importantly, they are provided with information about the entity with whom they are transacting. Regardless of whether the seller is an individual or business, the buyer can see how previous customers have rated that seller. They can see comments from other buyers about the quality or efficacy of their product or service. The buyer on Amazon or eBay is making an informed decision with whom they are conducting a transaction, so why can't a buyer using a faster payment option have the same or similar information that would power a similar informed decision?

Suppose that all of the information that is being gathered on reported bad receivers were consolidated into one database. Let's further suppose that the resulting database would be available to all vendors providing a user experience for initiation of faster payments to access, enabling the information to be displayed to the customer BEFORE they click to push a credit. Similar to how the Specially Designated Nationals list is used for OFAC checking on wires and ACH, this bad receivers list would only flag a receiver as "suspect." The customer would be able to see information on the receiver that, at a minimum, would indicate the number of reported fraud / requested return incidents. The application user interface might even highlight reported fraud as a part of the "Are You Sure" messaging to the customer. By providing meaningful information to the customer before a credit push is initiated, the option to significantly remediate APP fraud is introduced.

Let's return to the earlier example about the customer in Florida contracting to buy a dog. Upon entering in the contact information on the breeder, the customer sees on their app that the breeder has seventeen reported incidents of fraud / return requests. There is a link that allows them to see additional information that represents comments about this receiver, including any attempts to obfuscate any previous bad behavior by changing company names or other identifying information. Armed with this information, the customer elects to not push the credit and instead calls the breeder to inquire about the negative reviews and multiple incidents of suspected fraud reported. Could the company be perfectly fine and have reported incidents? Of course! But because Amazon and eBay empower buyers to know about reported bad actors, individuals and companies that use those platforms go out of their way to maintain a clear record. Further, if there is a complaint, they immediately take action to remediate the issue with that customer.

Could someone pushing a credit to an entity with no reported suspect fraud incidents get burned and be the target of fraud? Of course. Perhaps the information on how many inbound transactions an entity has received could be provided. A company that has 500 reviews and no reported fraud sounds like a solid bet. A company with little to no activity at all may just be starting out, and the customer may elect to take a chance that the transaction will work out fine. As with everything, there is always a risk in conducting business with any individual

or company, but overall, providing a consolidated view of reported suspected fraud to customers before they initiate a push credit is the best mediator of APP fraud.

Why Does the Suspect Receiver Database Need to be Comprehensive? – Companies offering an option to initiate faster payments can deploy their own methods of alerting customers of suspect bad receivers. Banks like Wells Fargo, Bank of America, Citi and Chase can each maintain a database of their own customers who have reported fraud. The Federal Reserve, The Clearing House and Early Warning each have their own database of suspect bad receivers. Vendors who produce the apps that drive push credits like Jack Henry, FIS, Fiserv, Q2, et al also can store information on reported bad receivers. In order to provide customers who are initiating a push credit via a faster payment solution important information on the receiver to whom they are directing a push credit, a comprehensive solution must be deployed. One entity must not only be the repository of all reported suspect fraudulent receivers but also makes that information available to all entities that are in a position to use it in support of reducing APP fraud.

Fraud Suspect Information and the Fear of Lawsuits – Entities like the Fed and The Clearing House are keeping tabs on known bad actors but will not allow any originating FIs to have access to this critical information due to "privacy." Private entities such as JHA, Fiserv and FIS are unlikely to report any suspect bad receivers due to the potential for lawsuits from companies that are included on any such lists. Further, receiving FIs may be hesitant to take any action against a customer who receives return requests or who are flagged by sends as fraudulent. The receiver might just say that the sender received exactly what they contracted for. How is the receiving FI in a position to monitor its customers in the absence of specific returns and chargebacks?

Therefore, it is likely that a government agency would need to agree to maintain the database of suspect receiver fraud and make it available to all faster payment recipients. The CFPB comes to mind as a logical choice for serving in this capacity. It is solely focused on protecting consumers from bad actors, and the proposed bad receiver database falls squarely in line with that mandate. Moreover, it would be an excellent opportunity for the CFPB to collaborate with the banking industry to solve a specific problem. Further, the availability of the database and the subsequent legal requirement to make its information available to receivers in advance of a push credit transaction would obviate the need to add APP fraud to Reg E. Customers would be able to make informed decisions and FIs who have given their customers the ability to make informed decisions would not be liable for potential bad choices that are outside of the FIs control.

Conclusion – Approved Push Payment fraud is an issue that deserves a thoughtful and measured response. By providing the information most useful in identifying a potentially fraudulent receiver in the hands of senders prior to them executing an irrevocable push credit, the industry would take a giant step in providing consumers with meaningful fraud mitigation. Due to the fractured nature of the payment systems involved and private sector concerns about the privacy of customer data, a government initiative to compile a comprehensive database of suspect bad receivers and the associated legal requirements for Sending FIs to

incorporate the information in the database to be made available to senders is needed. Based on its mandate to be a consumer advocate related to financial services, the Consumer Financial Protection Bureau may be the logical choice to create and maintain this database.

7813 Office Park Blvd, Baton Rouge, LA 70809
(225) 924-8015