Zelle Fraud

Top Ten Controls Banks Can Deploy Today to Protect Consumers

BioCatch

WHITE PAPER

There is currently much discussion in the U.S. about reimbursement for authorized payment transaction scams, especially around P2P and Zelle® type transactions[1]. The Consumer Financial Protection Bureau (CFPB) will soon come out with its commentary on how reimbursement to customers should be applied in such circumstances. Equally as important is how banks can mitigate the risk of these scams in the first place. In the UK, once the large banks started to reimburse for their equivalent of authorized payment transaction scams (called Authorized Push Payments or APP scams), they created and deployed new controls to help prevent these scams from even occurring.

It is important to first define unauthorized and authorized payment transactions. Financial fraud and scams are often classified into two distinct categories: unauthorized payment transactions and authorized payment transactions. An unauthorized payment transaction is done by a third-party criminal, such as an account takeover (ATO). There could also be a scam component to an account takeover where the criminal convinces a customer to provide the one-time passcode (OTP) required to complete the authentication. On the other hand, an authorized payment transaction is where the criminal uses social engineering tactics, often impersonating the bank or a government official, to get the customer to perform the transaction.

Financial institutions are required to provide reasonable commercially available security to its bank customers. This is the hallmark of the original FFIEC Guidance on Authentication in an Internet Banking Environment (originally published in 2005; updated in 2021). To help banks assess what additional controls to add to help prevent P2P/Zelle fraud, the recommendations in this paper will focus on authorized payment transaction scams. This list of controls is beyond the existing controls that most banks have in place today.

Before considering controls, it is important to understand the unique ways that banks process Zelle transactions.

- Large banks, and those that are more sophisticated, may develop their own Zelle screens, along with most of the Zelle fraud controls and do a direct interface to Early Warning Services (EWS), the network owner and operator of the Zelle platform. EWS also has fraud security controls.
- Regional banks and credit unions are likely to use a third-party technology provider (e.g., Alkami, Fiserv or Jack Henry) for the Zelle platform, or in some limited cases, they create their own Zelle screens and do an API to their technology provider. In this case, whichever entity owns the Zelle screens is generally responsible for most of the fraud controls. The third-party provider will then do a direct interface with EWS, which again has its own fraud controls.

Some of these recommended controls may be a better fit for large banks with greater scale and a need to have a more tailored product configuration and/or refined controls compared to the third-party intermediary platforms who create a more "plug and play" standardized integration to EWS. However, all parties involved should invest in elevating best practices for their customers and engaging in frequent customer education to enable the end user to mitigate some risk. Also, these controls are focused on the Zelle network solution (e.g., FIs having Zelle within their online banking platform) and not the Zelle common mobile app.

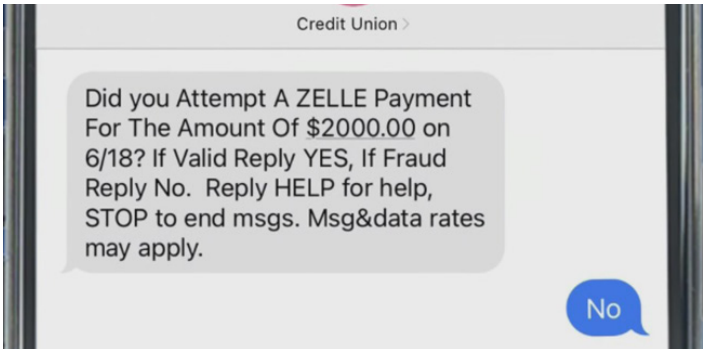
1 Refer to *Authorized Payment Fraud: A Global Guide to Customer Reimbursement Models for Financial Scams*

Unpacking a Zelle Scam

In September 2022, EWS issued a press release on Zelle that stated, "In the past five years, consumers and businesses, small and large, have sent more than five billion Zelle payments, totaling nearly $1.5 trillion." EWS also noted that more than 99.9% of payments were sent without any report of fraud. But this means there were up to .1% or 10 basis points, of Zelle transactions that could have been fraud (e.g., account takeover transactions) or a scam (authorized payment transactions directed by the scammer). This is up to five million transactions, or potentially up to $1.5 billion worth of fraud, over the past five years.

A subset of these approximately 5 million transactions are related to authorized payment scams. One of the key Zelle attack vectors, known as a bank impersonation scam, is described below:

1. The scammer sends out a significant number of text messages to a bank's customers claiming to be from the fraud department and stating that a Zelle payment attempt was made from their account. The text message often creates alarm or panic in the customer which prompts a reply. See example below.



2. The customer replies NO to the text message.
3. The scammer immediately calls the customer's mobile number (tied to the text message), pretends to be an official from the bank's fraud department (sometimes as an authorized third party) and convinces the customer into performing a bogus "reverse Zelle" transaction. This involves the customer thinking they are doing a 'me-to-me" transaction by sending the Zelle transaction to the customer's own mobile phone number (the Zelle token) to reverse funds sent in error.
    a. Note: there is one twist to this. The customer sees the text message and they take the initiative and actually call their bank. Because there is a backlog in the call center, the bank automatically offers a call back and the customer agrees. But before the bank calls back, the scammer takes the initiative to call the customer. The customer then really thinks it is the bank talking to them.
4. The customer does an 'authorized' Zelle transaction (the customer, not the scammer, executes the transaction).
5. The money immediately moves to the scammer's bank account.
6. The scammer hangs up.
7. Later, the customer realizes they have been scammed, and they call their bank.

These scams have proven to be highly successful which has caught the attention of U.S. regulators. However, banks have the opportunity now to take control of the narrative and set the course for better consumer protection relative to P2P payment scams. Following are the top 10 controls banks can embrace today. *(NOTE: This paper focuses on Zelle, but much of this could be applicable to other P2P apps such as Venmo and Cash App. When the CFPB comes out with their commentary, it will, at minimum, likely address all P2P services in the U.S.).*

CONTROL #1: Smart education close to the transaction

Everyone acknowledges that customer education to prevent fraud and scams is important. The regulators expect it. And everyone acknowledges it doesn't work well, with customers mostly ignoring it. Thus, banks need to rethink how customer education is rolled out. Scammers are very adept at deploying psychology to influence the actions of the customer. In turn, banks must deploy the same strategy when thinking about customer education to influence the customer to stop what they are doing during the scam. This is difficult because the scammer is already 'in the head and mind' of the customer, weaving believable stories. Customer education needs to focus on how to 'break the spell.'

How do we do this? The first step is to learn about the psychology of influence. A good place to start is with Professor Robert Cialdini's book "Influence: The Psychology of Persuasion." Unlike scammers, the goal of the bank is to influence the customer for the good. Dr. Cialdini even has a company, Influence at Work, that helps craft text to positively influence situations. Another interesting book, "The Psychology of Fraud, Persuasion and Scam Techniques" by Martina Dove, discusses how people fall for scams and the techniques used by scammers.

There are several ideas to influence customers with education:

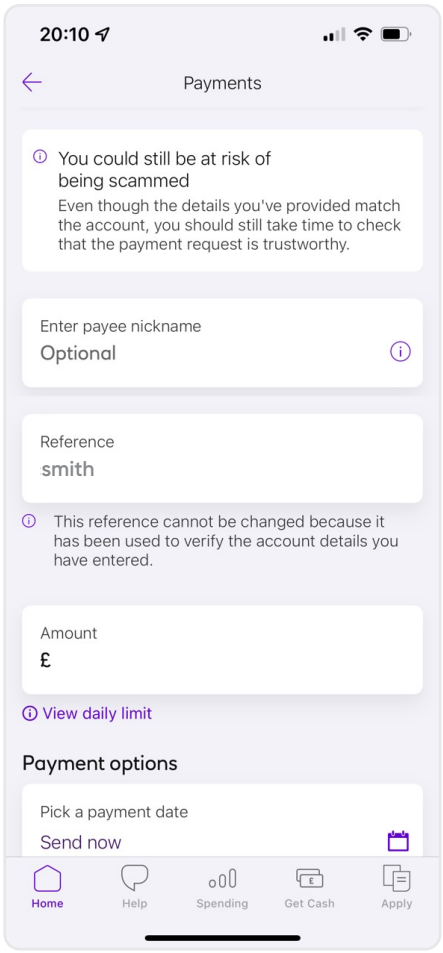
- Introduce an interactive education message for the first new payee. The pop-up type message will have content confirming the intention of the customer and require the customer to click a box to acknowledge they read it. The key message could be highlighted in red to capture the customer's attention or there could be helpful points for the user to acknowledge (e.g., "I know this person I am sending money to") and each point requires a click or check the box.
- Introduce a second interactive message if a large payment is being made to the first or second new payee. This is where the bank can introduce a positive message about protecting their customer. For example, the message could say, "Is a person on the phone directing you to make a Zelle transaction? If yes, this could potentially be fraud. Immediately hang up and call the toll-free number on your bank statement." The use of color, bold, CAPS and adding exclamation points in the message can be helpful.
- Introduce smart interactive educational messages on the Zelle platform on a periodic basis, maybe every 3-6 months. For example, a message might read, "Did you know that most Zelle fraud scams start with a fraudulent SMS text message to your phone?"
- Push messages in unconventional locations close to, or in context around the transactions, distinct from other notifications/message types have a greater impact. Seek to make in-app "push messaging" possible and pertinent to the user journey.

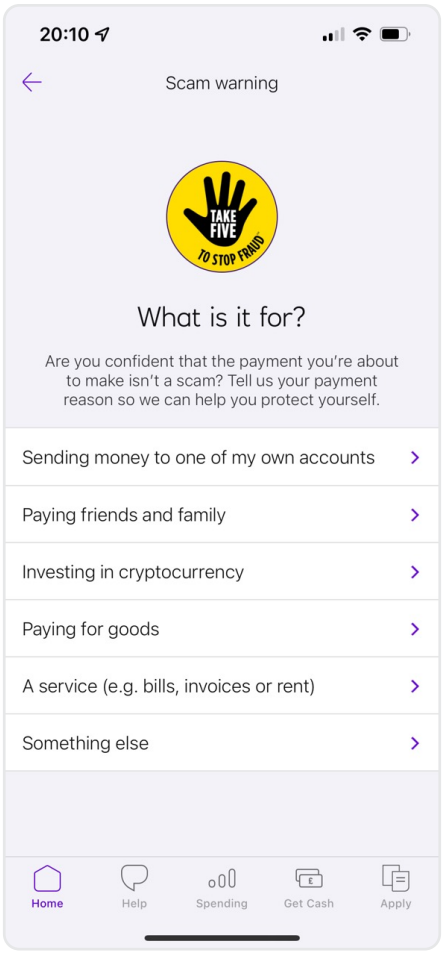
Take time to craft these educational messages and how they are delivered so they truly influence the customer. Otherwise, it is a waste of time.

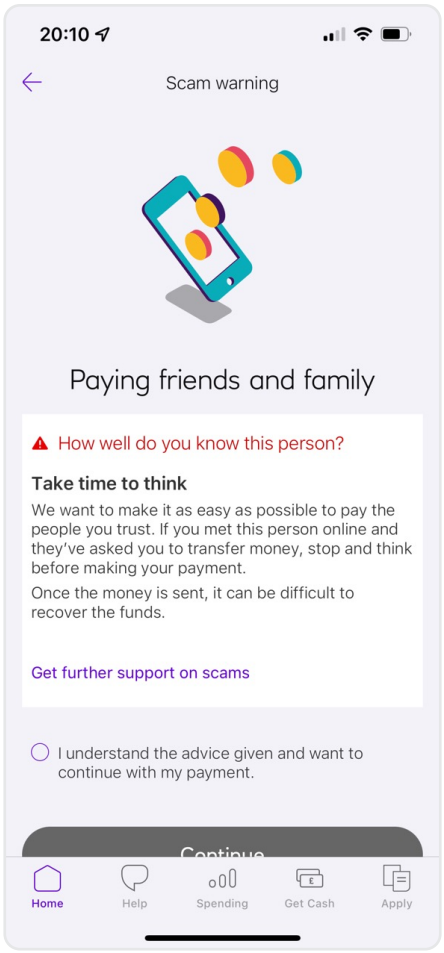
"Scammers are very adept at deploying psychology to influence the actions of the customer. In turn, banks must deploy the same strategy when thinking about customer education to influence the customer to stop what they are doing during the scam."

CONTROL #2: Transaction nudges

A 'nudge' is a simple behavioral intervention to induce an action. A transaction nudge, which first began in the UK, is a message to the customer at the time of a transaction where the bank sees something anomalous about the transaction. The 'nudge' message is crafted specific to this transaction and the anomaly. The purpose is to get the customer to stop and think about what they are doing. During the scam, the intent is to get the customer to stop the transaction, hang up on the scammer and call the bank. Here are some nudge examples below:







CONTROL #3: Delay execution of payments for new payees

Banks have the right to delay transactions if there is a concern about fraud. A customer making a high value payment to a new payee, especially the very first payee, has high risk associated with it. Checking the phone number or email token is not good enough as the scammers can assign this legitimate token to their money mule bank account during the scam. A good rule to follow for a new payee, the first Zelle payee, or additional new payees where the payment amount is over a certain threshold, is to delay the payment for a short amount of time (as determined by the bank). This delay can also be based on the customer's own transaction payment history, and banks can take into account the customer's age (as part of an Elder Abuse Program or other program focused on vulnerable customers).

It could also be appropriate to delay transactions if the mobile phone number or email address has just been established with the mobile carrier/email vendor. As an example, this could help catch a scammer having a customer send a payment to a lookalike email address (e.g., charles.smith@gmail.com vs. the correct charlessmith@gmail.com).

Do this even if the customer passes step up authentication (e.g., an OTP authentication) as that could just be part of the scam where the customer receives the OTP and provides it to the scammer who then uses it to successfully complete the challenge.

A four-hour delay is recommended as that allows enough time for a scammer to disengage with a customer (the phone call ends), the spell to be broken, and the customer to call the bank to say they were scammed. In this time, the money has not left the customer's bank account. This delay tactic has proven to be very successful in the Netherlands.

Another option would be to put control in the customer's hands to delay the payment for a specified period of time. Any change to this option has a one-day delay. Perhaps the delay control is set as the default at Zelle setup. This delay control should have a value limit (e.g., delay if payment is greater than X amount). Typical low-value transactions would always go immediately.

There are several considerations to address before implementing transaction delays:

1. Work closely with the bank's Risk Manager, Digital Channel Manager and the Marketing Department. There needs to be a clear understanding and agreement as to why these delays should take place: PROTECTING THE CUSTOMER.

2. When implementing a delay of transaction control, take into account the hours of operation of the call center and fraud department. If a bank is not running 24x7 call center support, consider limiting transaction delays to when the call center is operational.

3. Be aware of any EWS guidelines/SLAs on transaction delays. These delays should only occur because of identified fraud risks. The Zelle network operating rules require the customer be notified if there is a delay in the processing of the Zelle transaction. Notification could be an online notice – an email to the customer or a phone call from a bank fraud analyst. The customer might still be on the call with the scammer and then tell the scammer about the delay and be given instructions on how to 'handle' a call with the call center.

CONTROL #4: Look for 'me to me' transactions

This control is to prevent the scammer from using the customer's phone number or email address as a token at the receiving bank. This can make it look like a 'me-to-me' transaction to the customer. Thus, the control needs to alert when the customer's phone number and email address are used at the receiving bank. A real customer can have two bank accounts and the customer's phone number and email address can also be used at the receiving bank. It can be common for customers themselves to move the phone number or email address between banks (e.g., a quick delete and add of the same token).

Some additional rules for this control may be required:

- Check if the Zelle token used for this payment was deleted and added in past 30 minutes. This control is looking to catch the scammer having the customer remove their phone number as a Zelle token and then the scammer adds the same phone number to their bank account. Note: On its own, this is not a good control because sometimes customers themselves will move one of their phone numbers to another bank-owned account.
- Check if the customer's phone number and email address were also set up for tokens at the receiving bank in the past hour before the actual transaction. Include ownership assessment of the phone number and email address.
- Conduct a basic match on the name and address of the sending and receiving bank. This should identify that the receiving bank account is owned by the customer at the sending bank. If this match is positive, it is probably the real customer.

Two possible alerts:

- Create an alert if the same Zelle token was deleted at sender bank but added at the receiving bank, all within the last hour, and if the sending customer's owned phone number and/or email address is used as a token at a non-owned receiving bank account.
- Create an alert or nudge if the sending customer's owned phone number and/or email address is used as a token at a non-owned receiving bank account. For example, the nudge might say, "The payee mobile phone number/email address is associated with you, but a) it is linked to a different account at your bank or b) it is linked to an account at a different bank. Is this what you intended?"

If the scammer is adding the customer's phone number or email address as a Zelle token at the scammer's receiving bank, the IP address used for the token setup at the receiving bank will be different than if the actual customer was adding a new token at another bank (also the receiving bank). A more sophisticated network control would be to look at the IP address at both the sending and receiving bank when the same token is deleted and quickly re-added. For example, you would see the actual customer online at sending bank A with IP address 44-098-0976-09 and the scammer is online at the receiving bank with IP address 7654-98-0098-09. If the IP addresses are different, then create an alert.

Also, if the above conditions are met, and a payment is initiated greater than a certain threshold determined by the bank, the payment could be delayed.

CONTROL #5: Do Confirmation of Payee check

The purpose of a Confirmation of Payee check is to tell the sender who the payment is really going to. In Zelle and other P2P transactions, the payor is sending money to a payee identified by an email address or a phone number. As part of the transaction, the system should be able to show the payor (the customer sending the money) that the name (when a payor set up a payee) on the payee token is the same name on the bank account receiving the funds. Because of privacy, this is typically done via a matching process. There are several issues here:

- From a bank privacy standpoint, only so much of the receiving bank's customer name can be shown.
- Currently, Zelle only shows the sending customer (payor) the first name of the person who enrolled the Zelle token being used as the payee. This name comes from the bank that does the Zelle token enrollment.
- The receiving bank account, where the Zelle token is registered, may be a joint account.
- The receiving bank account may be in the name of a company.
- This solution may not be able to list the name of the receiving bank, but it could show if the receiving bank is different than the sending bank. Note: if this were a true 'me to me' transaction, then the bank name for the payee would be the same as the bank name for the sender. This could alert for all cases, except where the scammer has a money mule account at the sending bank itself.

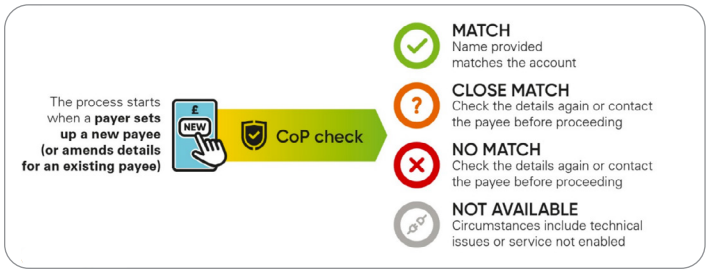
Keep in mind, for other real-time payments, such as a wire or ACH, the customer is sending an amount to a specific name and another bank. In this instance, Confirmation of Payee is easier to execute.

The first example to the right shows a Confirmation of Payee in the UK.

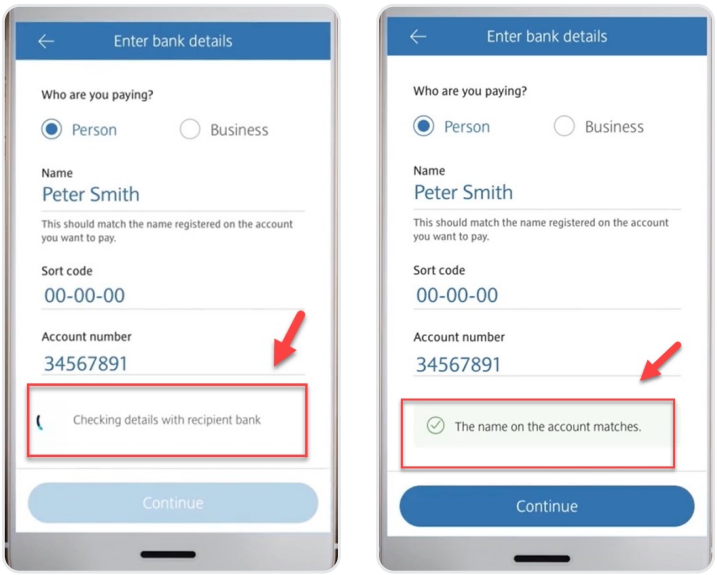
The second example to the right shows what a Confirmation of Payee looks like from the customer side.

Some solutions for this are as follows:

- In the example of the wire, the system should be able match the sending name to the name on the receiving account and return a "match, partial match, no match." This is like the Confirmation of Payee in the UK.
- For Zelle transactions, the system should be able to return at least the first names of the account at the receiving bank. For Mary and Tom on a joint account, it should not only show Mary, or the first name on the account. If the receiving account is a company account, then show what is allowed from a privacy perspective, or state it is a company account (or non-consumer account).
- A better solution for Zelle would be to create a true Confirmation of Payee solution using the name the sender inputs for the payee token and matching it to the name on the payee's receiving bank account.



Source: Pay.UK



Source: Barclays

CONTROL #6: Check if the customer is in mobile phone session

This is a new control that is currently being tested in the UK. In a majority of these scams, the scammer is on a call with the customer on the customer's mobile phone (matching the mobile number associated with the smishing text message), impersonating the bank to get the customer to perform a Zelle transaction. The scammer 'telephone engagement' can also be true for the IT help desk scam and other scams, as well.

As another point of information, here are some things to check for when a customer is performing a transaction. (NOTE: It could also be beneficial to do this check at log in).

- Is the customer's mobile phone in a session?
- Is it an inbound call?
- Is the call duration long?

If all three rules are positive, this could be indicative of a scam situation. Take action with a nudge or a hold for call/fraud agent review. Also, make sure the rules results are in the case manager for the call agent or fraud analyst to have available if the customer or scammer calls to follow up.

DID YOU KNOW?

75% OF SOCIAL ENGINEERING SCAMS TAKE PLACE IN THE MOBILE CHANNEL

(Source: BioCatch)

CONTROL #7: Make the default setup option for Zelle=NO

Customers should be required to set up Zelle service. Add some friction along with interactive education. Do not make it a default=YES. Opt-in rather than Opt-out.

Tied into this control at setup would be to delay a large payee transaction for four hours or longer. This is not just for the first new payee, as the scammer may try to do a small dollar amount for the first new payee, then do a larger amount for the second new payee.

The bank's marketing department may not like this control at first. However, if it can be tied to customer protection and building customer trust, it will be easier to get buy-in.

CONTROL #8: Look for signs of stress, distraction or hesitation by the customer during a transaction

One of the more interesting controls is to observe the behavioral biometric responses of the customer while doing the real-time transaction. Even if it is a genuine customer making a payment, when a person is acting under the influence of a scammer, there are subtle changes in behavior that can build a picture of a user's emotions or intention during a session and suggest a scam may be in progress. For example, a key sign that a customer is distracted is excessive mouse doodling. This behavior is logical given the long waits, pauses and dead time caused by a scammer explaining or dictating instructions to a customer or to keep an online session from expiring in the process. The average number of doodles across all confirmed impersonation scams is six. While only one percent of the general population exhibit six or more doodles in a session, that figure rises to 38% in reported fraud cases[2].

Several large banks in the UK have deployed this technology control with positive results.

2 Source: BioCatch

CONTROL #9: Detect unusual online session flow and behaviors

Session flows, or the tracking of the online user journey, can be strongly correlated with the potential risk for social engineering of a victim. Frequently, there is a script that the scammer will take the victim through, and this is a telltale sign for the subsequent transaction.

By way of example, some scams lead the customer to realize an account has a higher balance than they expect to have in an account, and in this situation, a transfer may have been made from another account the customer possesses. Perhaps originated from a credit card or line of credit advance, if not another account which may possess a quality of the balance being more obscure than the primary depositary account. Seeing a recent transfer may provide some context to the potential that there is a high-risk event forthcoming.

Leveraging this, as well as some of the other behavioral biometric signals, such as mobile calls in session and the changing contexts of the device (from a vertical to a horizontal device orientation) can indicate that a user is picking up and putting down a device to view the screen which may be a strong positive correlation to an active social engineering event.

CONTROL #10: Utilize third party integrations such as the Zelle Risk Insights program to inform your alerting decisioning strategy

Many of the P2P networks recognize that there are ways that they can provide additional risk indicators that can be leveraged in the decisioning process. These can be ingested into risk decisioning engines, and they can be extraordinarily powerful in the context of the payment. This may work in a similar capacity as Confirmation of Payee but extend the power of the value this data offers by an order of magnitude.

Consider isolating actionable variables that contain risky elements relative to the beneficiary, such as their legitimacy and their length of time on file. More mature beneficiary accounts are more likely to be reliable in contrast to accounts with low time on file or a low volume of received transactions.

Leveraging any of the scoring models provided by third parties and ingesting these into a consolidated/ orchestration fraud solution can be a winning combination.

“Behavioral biometric signals, such as the changing contexts of the device (from a vertical to a horizontal device orientation) can indicate that a user is picking up and putting down a device to view the screen which may be a strong positive correlation to an active social engineering event.”

The Power of the Ecosystem

Banks can do a lot to mitigate risk by taking the previous steps, but there are other entities within the ecosystem that are important in the fight against fraud, specifically mobile carriers and receiving banks. Following are two critical ecosystem controls to consider.

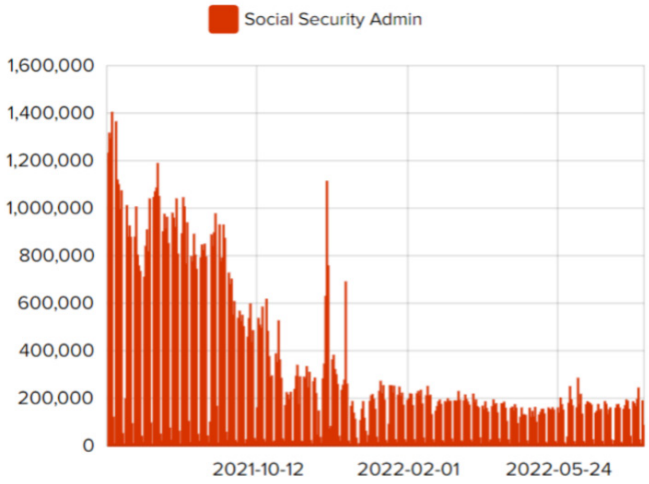
ECOSYSTEM CONTROL #1: Prevent text messages and phone calls from being spoofed as coming from banks

Banks need to work with the mobile carriers and other key participants in the telco ecosystem, such as iConnectiv and the telco trade association US Telecom-The Broadband Association (and its Industry Traceback Group-ITG affiliate), to build out a way to prevent scammers from sending text messages and phone calls that appear to come from the bank (commonly known as spoofing). For text messages, this can also involve working with Apple and Google (for Android), as they have a certain amount of control over the text messages in their mobile operating systems.

It can be very difficult to block spoofed domestic telephone calls coming from overseas (really the bulk of these calls) or from non-fixed VoIP numbers because the scammers are smart enough to route the calls initially via TCP/IP and software until the phone calls gets within the U.S. And only then does the call start to go through the U.S. telco system. Blocking spoofed domestic numbers inbound to the U.S. can also be a problem as there are many legitimate bank call centers in Canada, India, etc. Some industry experts have observed that spoofed calls are being replaced by scammers using real phone numbers. Detection must adapt to reflect this change.

Some ideas that are being discussed to help mitigate text message and phone call spoofing are:

- There is one vendor currently working with large U.S. companies to put an indicator on each legitimate text message. This could also force a different text stream for legitimate vs. spoofed text messages.
- Another vendor is able to identify bank impersonation calls being used against a financial institution and work with the Industry Traceback Group to get these calls shut down. This can be an iterative process, as calls are shut down, new numbers used and shut down, etc. Below is a chart showing the success of a recent shutdown campaign, similar to the bank impersonation case, that was executed for the US Social Security Administration (SSA). As these SSA impersonation calls were being shut down, the chart below shows the dramatic drop in actual impersonation calls.



Source: US Telecom-The Broadband Association presentation to the FCC on August 17, 2022

The Federal Communications Commission (FCC) in September 2022 proposed "to require mobile wireless providers to block illegal text messages, ...by blocking texts, at the network level, that purport to be from invalid, unallocated, or unused numbers, and numbers on a Do-Not-Originate (DNO) list."[3] According to the FCC, this will basically extend some of the FCC consumer protections against illegal phone calls (e.g., blocking illegal calls at the network level) to text messages. This proposal has been expected for a year. It gives the mobile wireless providers legal protections to block these illegal text messages.

3 FCC NOTICE OF PROPOSED RULEMAKING - Targeting and Eliminating Unlawful Text Messages, September 23, 2022

Some large banks are already focused on looking for and testing solutions to mitigate this impersonation spoofing component of these P2P transaction attacks. For example, Barclays has added the following control: "If we call you, ask us to use app ID to send a secure notification to your Barclays app. You'll be able to log in to your app to see the name of the colleague you're speaking to and you'll be able to confirm you've got the notification so we know it's you too."

ECOSYSTEM CONTROL #2: Create anomaly detection on inbound financial transactions to bank accounts to be able to detect and shut down money mule accounts

Several international regulators are realizing that weak controls at the receiving bank in a fraud or scam transaction are a major reason these activities successfully occur. Some regulators are also taking under serious consideration the requirement that receiving banks share in the reimbursement for these fraudulent transactions. There are a few banks in the U.S. and the UK that take this seriously and have mule attack teams. Every bank should take this seriously. And one of the best ways is to build anomaly detection on the inbound and outbound flows against the bank's accounts.

Money mule accounts look different:

- Much more inbound traffic from wires and P2P/real-time payments
- Transaction dollar amounts are high
- Outbound transactions are quickly done after the inbound transaction is posted
- Overall high velocity of inbound and outbound transactions is high

Tied into this is doing anomaly and behavioral detection on online login and account transaction activity. Scammers are constantly logging into money mule accounts to see if the funds arrived. That is not a normal behavior. Plus, the way a scammer navigates through the screens can be quite different than a typical customer.

The Zelle network can also be analyzing multiple high value transactions going to the same payee, as a sign of fraud or scam activity. But there is a need to look at payee account history, as it could be simply a landlord receiving high value rent payments via Zelle on the first of the month.

Receiving banks should have the real-time ability to alert and hold inbound transactions, if they believe there is a possibility of fraud.

NOTE: Money mule accounts are not all owned by scammers and could be a long-term existing customer account where the customer went rogue for money. Understanding the differences in behavior patterns can also help banks spot legitimate customers who may be using their accounts for the purpose of money laundering or fraud.

Cooperation on the part of sending and receiving banks can go a long way in detecting and removing money mules from the U.S. banking system.

The Impact to First-Party Fraud

After discussing these controls to detect Zelle payment scams, it is likely that banks could see a rise in first-party fraud claims in the future. This will be especially true if the CFPB rules that certain authorized payment scams must be reimbursed or banks start to reimburse these scams on their own volition (as is starting to occur today). Some of these same controls described above can help to detect first-party fraud.

1. Use behavioral biometrics to help detect if there is real stress being experienced on the part of the user completing the Zelle transaction. Or is it faked stress? Or does it just look like the real customer doing another Zelle transaction?
2. Use potential Zelle network capabilities. Is the same IP address and device print being used by the customer doing the transaction at the sending bank and by the person adding the payee at the receiving bank? Also, does the IP address used at the sending bank or receiving bank reside in any consortium data showing it as a known bad IP address?
3. Require proof. Can the customer show they received a spoofed telephone call from their bank at the same time the 'scam' occurred? This is part of the Dutch controls associated with bank impersonation reimbursements.

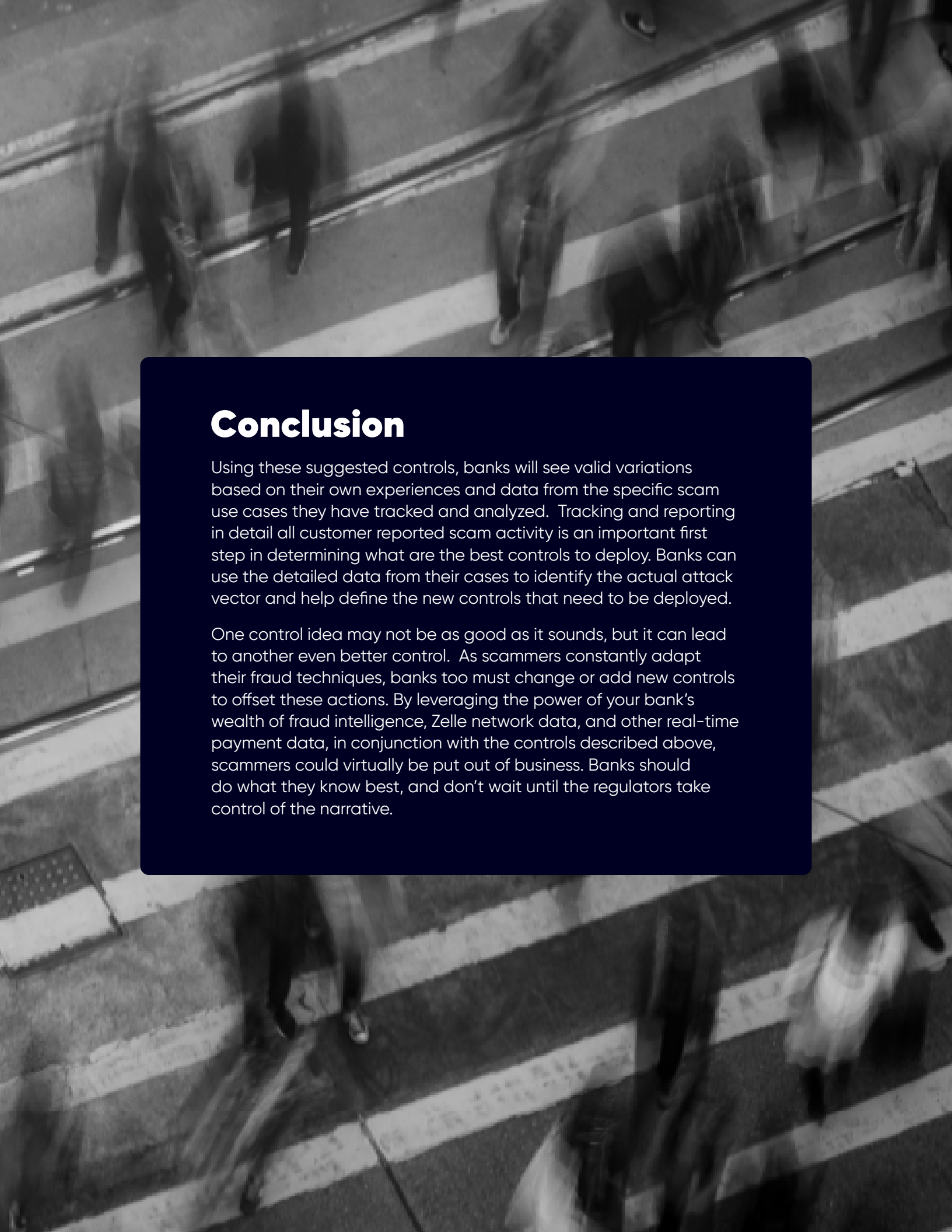
If the first-party scammer, your customer, is smart, they can possibly beat number 2 and 3.

The UK's Payment Systems Regulator (PSR) TechSprint Demo Showcase

In September 2022, the UK Payment Systems Regulator held an Authorized Push Payment (APP) Tech Sprint to help identify new controls to help mitigate scams around real-time payments. This involved a large number of participants broken down into teams for three days to come up with new control ideas. Some of these ideas discussed included:

- The use of more data
  - Telco data on calls
  - Behavioral biometrics
- Integration with the receiving bank
  - Send risk score to receiving bank
  - Receive risk from receiving bank
  - Conduct confirmation of payor with receiving bank customer
- Use open banking platform to obtain more data
- Have more targeted nudges
- Do confirmation of payee with crypto companies
- Getting social media companies to provide alerts when bank account information is being shared, especially when one account is receiving many bank account details (difficult with encryption on some of these platforms)

The PSR exercise shows that when interested parties come together, serious ideas can be generated to help solve the scamming of bank customers around real-time payments.



Conclusion

Using these suggested controls, banks will see valid variations based on their own experiences and data from the specific scam use cases they have tracked and analyzed. Tracking and reporting in detail all customer reported scam activity is an important first step in determining what are the best controls to deploy. Banks can use the detailed data from their cases to identify the actual attack vector and help define the new controls that need to be deployed.

One control idea may not be as good as it sounds, but it can lead to another even better control. As scammers constantly adapt their fraud techniques, banks too must change or add new controls to offset these actions. By leveraging the power of your bank's wealth of fraud intelligence, Zelle network data, and other real-time payment data, in conjunction with the controls described above, scammers could virtually be put out of business. Banks should do what they know best, and don't wait until the regulators take control of the narrative.

About BioCatch

BioCatch is the leader in Behavioral Biometrics, a technology that leverages machine learning to analyze an online user's physical and cognitive digital behavior to protect individuals online. BioCatch's mission is to unlock the power of behavior and deliver actionable insights to create a digital world where identity, trust and ease seamlessly co-exist.

Today, BioCatch counts over 25 of the top 100 global banks as customers who use BioCatch solutions to fight fraud, drive digital transformation and accelerate business growth. BioCatch's Client Innovation Board, an industry-led initiative including American Express, Barclays, Citi Ventures, and National Australia Bank, helps enable BioCatch to identify creative and cutting-edge ways to leverage the unique attributes of behavior for fraud prevention. With over a decade of analyzing data, more than 70 registered patents, and unparalleled experience, BioCatch continues to innovate to solve tomorrow's problems.

For more information, please visit www.biocatch.com

This paper was written and researched by Ken Palla of Palla Consulting and sponsored by BioCatch with special contributions by Seth Ruden, Director of Global Advisory at BioCatch.

BioCatch

www.biocatch.com
E: info@biocatch.com
@biocatch
/company/biocatch