Alacriti

Navigating Fraud in the World of Instant Payments: Strategies for Success

With so much change within payments in recent years, there has been a corresponding change in the amount of regulatory scrutiny and considerations for fraud prevention. In particular, existing fraud prevention systems must be augmented to accommodate the new requirements of instant payments.

In a Banking Exchange hosted webinar, Mike Cook, VP of Commercialization, Fraud Solutions at Socure, and Mark Majeske, SVP Faster Payments at Alacriti, discussed the current and future state of fraud in the instant payments landscape, as well as strategies for protection to combat evolving fraud trends.

Synthetic Fraud

An interesting fact about Mike Cook is that he actually came up with the term 'synthetic fraud' in 2002 while doing research during fraud investigations. While looking at applications, he noticed that not only were a lot of the fake identities coming from the same household, but the names would look the same, and the social security numbers would all have an identical base in the number. Cook then went on to sit on the task force the Fed created to put a definition on it. Synthetic fraud boils down to creating a fake identity for financial/personal gain.

There are different kinds of synthetics, and they each have different motives. Cook explained, "The most important thing to know is you've got fabricated synthetics that are just completely made up. You can go to the internet and do random name generation, create a date of birth, and build a social from a random social or try and tie it into a real social. You can actually build a fabricated identity. The other type of identity is manipulated synthetic. That's when you are who you say, but change your identity in such a way that your old credit report can't be found. The issue with a manipulated synthetic is that the decision you're making is off the wrong credit report. So you tend to under-assess the risk."

It used to be that fraud changed every six months, making having a model upgrade once a year or two an effective strategy. Then fraud began changing monthly. Now fraudsters can even make intraday changes to their target efforts. For example, in the morning, they may use information (name, social, etc.) they've gotten from the dark web, and they'll apply. Then they will use a fake number because they know the financial institution is uses OTP (One-Time Password) to validate the phone number. They will start changing emails mid-day because they think the financial institution will switch from OTP to email registration. These types of quick changes make fraud very dynamic. The fraudsters will also test the financial institution's system a lot—mobile, PC access, physical location, etc.

In addition, Socure is seeing some fraud increasing in physical locations because financial institutions shifted their focus to virtual activity because of COVID. Cook advised financial institutions to test themselves and keep in mind that fraudsters will always take advantage of anything new that they do. "Fraudsters have an amazing amount of better tools than they did three years ago. And those tools could be, 'I'm going to rent a server, and I'm going to use your server to run all my fraud through. I'm going to use open-source bots'. There's so many forms to get information, providing fraudsters with the opportunity to have a lot of data. Stopping fraud is harder than it's ever been in the 36 years I've been in the industry."

Money Mules and Tomorrow's Fraud Prevention

Majeske shared his experience from working in banking. "When I was working at banks, a fraudster would launch an attack, and obviously, we would make changes to our model. Once we did that, they would go away. And I'm thinking they just went away to another bank that was easier. So this is an ongoing process. Fraudsters don't go away—they just go somewhere else."

Cook shared that Socure is hoping to build in their next iteration of technology, the ability to predict where the fraud attack will go next. He also observed that money mules are always the lowest on the list. The reason is thought to be that not only is there not necessarily a loss to the financial institution, but they also fall under the radar and are not easily detectable. "Today, the consumers take the financial loss that happens. They have to take that loss on themselves from a scam, especially through Zelle® or any other P2P. And so we see a change coming right from the regulatory groups and even maybe the banks using self-regulation and taking these losses as a competitive advantage. We're talking to our customers about the Consumer Financial Protection Bureau (CFPB) and the focus on putting the losses back to the banks on a P2P scam, even though the consumer is the one who did it. It is going to have a major impact. Mules slip through because you missed them because your third-party cut was low at origination, you didn't have synthetic in place because you were relying on CIP (Customer Identification Program), etc. So you've got ATO (Account Takeover Fraud) happening and you're not paying attention to changes of address, change of phone, or other non-monetary changes. When that happens, it creates mules. And if we don't do something to identify those mules, that's where we're going to run into big problems."

Money Mule: A money mule is someone who transfers or moves illegally acquired money on behalf of someone else. Criminals recruit money mules to help launder proceeds derived from online scams and frauds or crimes like human trafficking and drug trafficking. Money mules add layers of distance between crime victims and criminals, which makes it harder for law enforcement to accurately trace money trails. Money mules can move funds in various ways, including through bank accounts, cashier's checks, virtual currency, prepaid debit cards, or money service businesses. Some money mules know they are supporting criminal enterprises; others are unaware that they are helping criminals profit.

Source: Federal Bureau of Investigation

Majeske remarked on his take on money mules. "When you look at instant payment rails, the majority of fraud we experience is through account takeover. But the second is mule accounts. If we are in a position as an industry to recognize a mule account before a transaction is sent, that's hugely valuable. Because regardless of what the regulatory environment is like, it helps the FI help the person. What if, for instance, someone comes into the bank and says she has to wire quickly to another country, and the system was able to pick up that it was a suspicious account that the money was being sent to?" For a P2P transaction, this could be accomplished by looking at risk scores for the email or phone number associated with the account.

Cook speculated that ATO will continue to be constant because of the availability of information on the internet. Especially considering data breaches that occur, revealing name, address, social security number, and date of birth. "They're not going to stop social engineering. They're not going to stop putting malware. They're not going to stop SIM swapping. They're going to continue to push on Account Takeover—especially in a down economy. If we see an economic downturn, ATO attacks are going to be pretty drastic. They really are the new money mule."

Social Engineering: Social engineering fraud is a broad term that refers to the scams used by criminals to exploit a person's trust in order to obtain money directly or obtain confidential information to enable a subsequent crime. Social media is the preferred channel but it is not unusual for contact to be made by telephone or in person.

Source: Interpol

Socure did research with their customers to understand fraud attacks post COVID. Surprisingly, there was quite a drastic change for synthetic fraud. While they still attack credit cards, auto, and personal loans, there was still a lot of money mule activity. Socure has seen an increase in first-party fraud. It appears that the stigma of committing first-party fraud has gone away, with people justifying it due to the economic downturn.

First-Party Fraud: What is first-party fraud? First-party fraud is where a person knowingly misrepresents their identity or gives false information for financial or material gain.

Source: Experian

Second-party fraud is a relatively new definition. In this instance, the first fraudster allows the second fraudster to perpetrate fraud through their account, and then the first fraudster tells the bank it wasn't them. Socure expects to see more of that happening. Especially if the dollar losses are taken on by the bank—consumers will see a way to take advantage of it. It's difficult to validate which individuals are actually victims.

Second-Party Fraud: What is second-party fraud? Second-party fraud is where an individual knowingly gives their identity or personal information to another person, to commit fraud. One of the most common types of second:-party fraud is money muling.

Source: Experian

Strategies to Protect Your Financial Institution

A layered approach to fraud detection is still recommended and was number one on Socure's list of recommendations. However, it used to be that the layers were rules. Cook explained, "The old school way would have been, the layers are rules. And you know what happened back then. It became unwieldy. You had like 80 rules in place at any given time. It caught so much fraud at a good false positive rate, but then those things go old. So you do need a layered approach, but I think it's good to have a vendor that you rely on. And you certainly want a model for every type of fraud that impacts you, as opposed to saying, 'I've got a fraud model. I'm covered.' Once you put a new process in place, fraudsters are going to attack and find a way around it. So it's constantly updating what you're doing." A layered approach takes into account more than one score and makes sure the scores work together.

It's also necessary to become an expert in friction. Fraudsters can give an identity with a real person, and as soon as they get approved, they go to the back end and change the address and phone number. However, you don't want to add a lot of friction to the consumer. The challenge is to apply friction to the consumer in a way they're used to. So, for instance, KBA (Knowledge-Based Authentication) is now an old technology where consumers have to answer a bunch of questions. Consumers today are used to a more modern approach, such as taking a picture of the front and back of the drivers license.

Passing signals forward, starting at origination, is a way to combat fraud while not increasing friction. While the fraud and synthetic scores may be marginal, it may not be necessary to friction the consumer. However, the signals should be passed forward to account management. So if they're doing a transaction that looks a little suspicious that they wouldn't normally elevate, they know to elevate it in that instance. "What I'm seeing is data—pure data from one system, sharing data with another. With faster or instant payments, it's a different kind of fraud detection than ACH and wire. Generally, what I'm seeing is banks have a separate enterprise system for ACH and wire. They ask, do I have to upgrade my current system to do instant payments? Because if I'm a bad actor in instant payments, I'm probably one in ACH and wire as well. And so the data helps the financial institution put the puzzle together," Majeske commented, "I like the instant payment models because you get the data so quickly. You're decisioning a transaction in milliseconds, not hours. So I favor taking the output data from the instant payment system and feeding it into the ACH and wire system, which benefits the organization as a whole."

Cook stated that the number one thing you can do is spend more money on model governance, as it will easily pay for itself. "Machine learning isn't what sets banks and solution providers apart. Everyone can do machine learning. What sets people apart is the ability to do a very efficient and good job of updating the machine learning models as rapidly as necessary to capture new signals and vectors and to implement that. The faster you can get those new models in, the better you're going to be able to stop fraud because it's so dynamic."

Alacriti connects financial institutions to instant payment rails. In speaking with financial institutions, Majeske noted a couple of things. "I think we have a lot of institutions with enterprise fraud systems that are great for ACH and wire, but can they decision a transaction in milliseconds and protect themselves and their customers before the transaction even goes to the FedNow^{SM} Service or RTP® network? What we've looked at is, can we add to the current enterprise fraud system so financial institutions can upgrade with the same company they have. And so we're taking that layered approach and partnering with Socure to offer a fraud solution that's specific to instant payments, but it can also do ACH and wire too, or at least communicate with your existing system to share that data."

Alacriti's solution automates instant decision using transactional analysis and scores consortium data. It's important to be able to leverage the data from other financial institutions as well. Customization of tolerance levels is also key, so financial institutions can adjust a tolerance level short-term but also provide an indication of what needs to be done long-term in a model to satisfy that. Full-featured activity reporting makes it possible to provide enough reporting on individual transaction information for both internal and external audits.

Questions from the Audience

What are some initial things we should be doing immediately to combat P2P scams?

Cook: For me it comes back to, there's money mules hiding in your account. We all know that today we don't do a lot to really aggressively attack those money mules. We might look at it from a transactional or perspective, but we're not looking at identity information. So one thing we're doing at Socure for our customers is batch runs where we can basically look at a portfolio and allow you to efficiently identify and weave these guys out within a course of two weeks. So we can do a batch screen, pull those records out, give you a treatment strategy, and hold these accounts until they call in and go through document validation or something to validate that they're not a money mule. Determine a great treatment strategy, try and do it as frictionless as possible, but find those money mules and get them out. It's important to note that KYC (Know Your Customer) and CIP (Customer Identification Program) won't catch synthetic and don't necessarily always catch third-party fraud. So you want to have those models on top of your CIP program.

Majeske: And that's where the layers come in. If you can do that in one system, it's extremely efficient. And the data's all tied together so you can look at the output and be able to react to it, and you really learn a lot.

Is there anything in particular we should look at with instant payments, or is the layered approach the same across all payments?

Majeske: It's account takeover and money mules activity. I had a question the other day: is RTP or FedNow safer? It's different—it's a different kind of transaction, and fraudsters are finding ways to infiltrate any way they can. So it's constantly moving. But I think targeting those two items and layers work very well.

When it comes to RTP fraud screening, do you start training off ACH fraud, or is there a better way to do it?

Majeske: This is something that I looked at when I was at The Clearing House because we have a lot of ACH data. Yes, you can start there because it is a transaction, it has a sender and receiver, and usually, the amounts are very similar. It's a starting point but not an endpoint. So if you're looking at creating your own models, and you have ACH data, personally, I would use it, but then as you start to do RTP transactions, you start to blend the two together.

Cook: My response is back to kind of blocking and tackling. Anytime you've got new fraud that you're trying to attack, the best thing to do is define it really well. There's so many times I've seen fraud investigation groups where they don't have solid definitions. What you end up with is a real mess because what you're defining as fraud and what you're building your models to target, or what you are assessing an outside vendor on—their value to stop fraud is based on muddy labels. Oftentimes I think we spend very little time focusing on how I'm going to label and define fraud. How do I make sure that I make all my investigators look at fraud the same way? I always go back to definitions and labeling really clean because then you can build fantastic models as long as you have good labels to target.

Is it really possible to get rid of false positives altogether when it comes to instant payments? Where do you draw the line between providing a real-time response or accept or reject to the customer versus reducing the payment request reject rates due to false positives?

Cook: I always try to figure out years in advance—what can we do to get ahead of fraud and just immediately make the answers a binary yes or no? And be right a hundred percent of the time? It's very difficult and requires a lot of data sharing, great model building, and clean targets, and you have to stay ahead of the frauds. I think the answer is—you'll never say ahead. You'll always have false positives. I think that we can get better and better and better. Where do you draw the line comes back to being an expert at applying friction. You have to determine where you're going to set that score cut-off. Then can I apply friction in a way that the consumer doesn't even necessarily see? Can I go out and pull a different score as part of a layered approach? If that comes out and it looks like it's still suspicious, and they're in the marginal category, can I then take that first transaction, run it through so that the next transaction, I can catch that one better? You have to constantly test and constantly change that line.

Majeske: From a transaction perspective, there has to be balance. It's not going to work for your customer to place an instant payments transaction, and two hours later, you tell them it went right. So you balance the ability to send back that confirmation very quickly. We're all consumers and know what we expect. But you have to marry it to

Mike's point that there are always gonna be false positives because there's that fine line. Trying to reduce that number of them is definitely what you want to do. And I also think balance between the rules you put in place, so you don't punish a good customer. There are many different ways to change tolerance levels or to look at different customer types or when they're sending. And that's another thing to think about in terms of tolerance levels. But it's a fine balance and it's not one that's easily achieved.

Do you expect the fraud to be greater or less for FedNow compared to TCH?

Majeske: I'll give my opinion. I don't think it'll be any different. The reason I say that is that the two systems are very similar. I know because I've worked with both entities and in designing them. RTP has been out for five years and has some 300 banks on it. But as use cases start to proliferate in the marketplace, that's when we're going to see the divide, and I just don't see it yet. One is not safer than the other. From a fraud perspective, I think they're very similar, and you should treat both the same.

Since the RTP network and FedNow both have credit push models and the Fed is creating a negative list, is that enough for fraud prevention?

Majeske: No, it is not. It's helpful, but it's not anywhere near enough. I believe in conversations I've had with the Fedthat they have plans down the road to augment what they've done. I can tell you that RTP doesn't have a list. We talked about that years ago. It's helpful, but it's not the end all.

Cook: I'll chime in just from an analytics perspective. Bad lists are best for using in a model to target what has been bad in the past (signals and behaviors). They're nice to have. But in production, they tend to be laggards behind the signals that created those bad items.

*To find out more about the need for fraud prevention when it comes to instant payments, watch the full webinar, **Navigating Fraud in the World of Instant Payments: Strategies for Success**, featuring Socure and Celent.*

WEBINAR PLAYBACK

Navigating Fraud in the World of Instant Payments: **Strategies for Success**

Alacriti's centralized payment platform, Cosmos Payments, provides innovation opportunities and the ability for customers to make smart routing decisions at the financial institution to meet their individual needs. Financial institutions can unify payment processing all in one cloud-based platform—ACH, the Fedwire Funds Service, TCH RTP® network, Visa Direct, and soon, the FedNow℠ Service. The Orbipay AIQ fraud solution is available as an additional feature of the Cosmos Payments platform. To speak with an Alacriti payments expert, please contact us at (908) 791-2916 or info@alacriti.com