AI LEADERS PODCAST
EP 71 AI, FRAUD & REAL-TIME PAYMENTS
TRANSCRIPT

Steven Bufferd [00:00:00] Those individuals who are on the front lines, who are processing payments, who have to be suspicious and aware about cyber and fraud threats, that awareness and training is invaluable.

David Jones [00:00:21] Hi and welcome to another episode of the AI Leaders podcast. My name is David Jones. I am the leader of our finance risk and compliance data and AI practice within North America. As you will catch momentarily, we have another David on the phone. I will refer to myself as Jones for purposes of today. I've got David DeLeon and Steven Bufferd with me today. Our topic is focused around real-time payments, fraud, and AI. David DeLeon is a managing director at Accenture. He leads our fraud and financial crime practice in North America. He's got extensive experience assisting financial service clients across the AML KYC sanctions fraud and regulatory compliance arena. And Steven Bufferd is a Managing Director at JP Morgan Payments, responsible for trust and safety product management. He has an over 30-year career at GPMC, largely focused on payment and security processing and product development. Trust and safety was recently established to protect the bank and help its key clients with use cases that provide protection services to them across. As we think about fraud in the industry, specifically we've got two openers that I'd like to highlight that I think set the table for how we wan to take forward this conversation. Number one, according to the FTC, the Federal Trade Commission, U.S. consumers lost over $12.5 billion in fraudulent schemes in 2024-11, marking a 25% increase from the prior year. According to the Federal Bureau of Investigations, adjusted losses due to business email compromises reached over $2.9 billion in 2023. The net of it is that both from a business standpoint and a consumer standpoint, material losses have occurred across the regulatory landscape and our banking customers. Before I go further into this, I'm going to reach out to both David and Steven and let them provide a little bit of depth as it relates to how we're seeing this play out in the market. David, would you like to start?

David DeLeon [00:02:22] Sounds great. And first of all, thanks for having us on here and looking forward to guiding in fraud and AI. You know, it's really an incredibly critical topic. And it's been a core focus in the industry. We've all experienced fraud events, either our personal or professional lives that continue to play a critical role in how financial institutions operate and candidly how we as individuals protect our hard-earned money. It's only increasingly becoming more complex in the industry as more complex and sophisticated technologies are enabling the next generation of fraudsters to commit more fraud. We're seeing that through some of the numbers that you mentioned. And it's also an incredibly interesting time in history as we see continued investment around new technologies and approaches to combat the sophisticated and evolving techniques that fraudsters are using. I'm excited to discuss more about the trends and challenges as well as innovation in this area and how that pertains to the financial services sector.

Steven Bufferd [00:03:31] Thanks, David and David. I appreciate the opportunity to join with you today and talk about this important topic. When we think about surveys that we look at the industry, AFP, the association of financial professionals, puts out a survey every year and one of the most recent ones talked about 80% of the organizations, this is on the wholesale side, reported having been targets of payment fraud, fraud activity and highlighted the per face of nature of this threat. We also look at groups like FinCEN, who recently reported during 2024 that when they look at SARs reports that are coming from the banks as part of their BSA reporting, 42% of those are SARs for around identity and identity fraud, and they've been actually warning banks about the increasing levels of deep fakes and deep tape videos and identity frauds that are taking place across the industry. So, I think across the different metrics that you will look at and measurements of insight, this is clearly a problem that those that are in the payments business and protecting and ensuring that funds end up with the right recipient, that fraud is something that needs to be at top of the list of their concerns. So, I’m looking forward to a good conversation this afternoon.

David Jones [00:04:55] Thank you for that, Steven and David, appreciate it. So, we'll work from a 101 level into a four-plus level, if you will. And just starting with some of the basics, introducing the topic around real-time payments and connections to scams. David, I'm going to turn to you first. If you could, let's just lay the foundation for the listeners in terms of A, what are real- time payments? And then B, how are we seeing those largely connected to consumer scams?

David DeLeon [00:05:22] Yeah, that sounds good. And real-time payments have come onto the scene and just exploded in popularity over the past, call it seven or eight years. And this would be what many of us are familiar with or referring to when we think about Zelle and other P2P payment platforms that are out there. The adoption rates around these platforms have just continued to increase. We're seeing about a 40% year-over-year increase. And really the driver here is that these real-time payment systems allow for immediate and often mobile-based transactions. And that's something that the consumer, you know, typically and more probably has and demanding. The problem is the rapid nature of these transactions are also making them quite appealing to fraudsters. So, a big part of the complexity here is the immediacy of the payments really benefits the fraudsters who are carrying out the various scams. By the time the victims recognize that they've been deceived by a fraudster, the funds are already gone. So, we're seeing scams across many different dimensions. And some examples are what we call authorized push payment fraud or others like spoofing or even romance scams that are becoming more prevalent. So, for example, an individual may receive a call from someone at a bank claiming to be part of their fraud department. They're informed of suspicious activity on their account that they need to transfer funds to a quote unquote safe account to protect their money. I trust the caller and send the transfer and then only later realize that the caller was actually a scammer and the money's gone. So, these are the kinds of scenarios, and there's many more that we're seeing where we have legitimate customers who are making, uh you know, and authorizing payments willingly, uh but only finding out later that, you know, they're the victim of a scam. And so, institutions that are out there having to contend with these competing dynamics of customers wanting minimal friction and instant. access to payments while also needing to then apply friction selectively to stop fraudsters and complex balancing act for many organizations that they're contending with.

David Jones [00:07:45] Thank you, David. I appreciate you sharing that. I think that helps bring it to life from a consumer standpoint. Steven, if you could, given your expertise area, if you can maybe take that and now move into the commercial domain and potentially even expand it into the global footprint as it relates to what's happening out abroad.

Steven Bufferd [00:08:00] Great. Thanks, David. I think some of the prevalent use cases that we see at events impacting our clients are things like business email compromise, account takeover, and some of the scams that you can read about in the press. Those are usually where we have a lot of our time and focus and attention. What we've seen is really kind of an increasing involvement within the payment industry around what the payment networks are doing to help in a responsive fraud and business email compromise. Some of the examples I would point out in the U.S. are things like Nacho, which is the ruling association around ACH payments is coming out with a fraud mitigation rule that will require companies and institutions that are originating transactions, as well as payment processors to introduce a fraud mitigation program to help reduce the events and having everybody within that chain of the payment process playing a role to try to prevent fraudulent transactions. We also see activities within, say, for example, the clearinghouse, the Fed. I think we referenced Azel earlier, so within early warning, those organizations that are implementing and exploring other industry solutions to help them protect against fraud. And then when you look beyond the shores of the U.S., we see various nations beginning to take actions to solve for fraud, particularly within the faster payment space. So, the United Kingdom has a requirement around confirming a payee or confirmation of payee for any of the wires or faster payment activity within the UK. In 2025, we expect to see the EU implementing a verification of the payee requirements and then similar initiatives that we're planning for as well within India, Australia, South Africa, and we know that there are pending changes within New Zealand and Canada as well. So, I think what you see, again, both within the United States and outside the United States as payment networks and payment providers looking to proactively respond to this threat.

David Jones [00:10:40] Thank you for that, Steven. I appreciate both of you laying the foundation for our listeners. Preventing fraud has always been a challenge, right? Due to the bad actors continuing to adapt their strategies. We saw that explode during COVID-19 and the number of digital transactions that were taking place. So, with the vast majority of fraud cases involving some form of deception. David, can you start to take us further down the road of what specifically are the current threats that are in the marketplace and how are we collectively working on solutions to work against those?

David DeLeon [00:11:16] Yeah, happy to, and maybe we'll focus on a few of the ones that are most emerging here on the scene. And candidly, it's a bit of the dark side of AI and how fraudsters are starting to use AI to create more sophisticated fraud threats. Steven mentioned earlier around deepfakes. That's one of the incredibly concerning developments that we've seen come on the scene. Maybe just starting with what a deepfake is, which is effectively leveraging generative AI to create extremely realistic but fake videos leveraging video content that can be procured from social media or other outlets and then using this to increase the effectiveness of scans. A scenario we might see is receiving a video call purportedly from a family member claiming they were in an accident and needing money urgently for medical treatment. The video looks just like your family member, sounds just like them and so you transfer the funds thinking you're helping your family member in a time of need and then only later discover that it was fake, and it was a scam. and the fact that the video looks just like the person that you know sounds just like them can be highly convincing.

And it prompts individuals to act and to send funds when they may otherwise know better. And it's some of these new kind of technological capabilities that processors now have access to are just incredibly effective in terms of getting individuals to actually send and authorize the funds. And it's not just videos. We are also seeing in other media types, such as emails, text messages, websites, to really support all kinds of different schemes, whether it's phishing attacks or social engineering attacks or even voice cloning. We're starting to see voice cloning, helping to target contact centers and gain access to customer accounts by manipulating call center agents. So quite a number of different schemes that are being used really using the fundamental and underlying generativity AI technology and then just applying it new and different ways. Steven, maybe if you want to add anything that you're seeing as well, your sign.

Steven Bufferd [00:13:41] Well, some of the things that we're seeing are you starting to see this mix of irrevocable payments and faster payments. So once the payment is actually left to the doors and gone out to the recipient, then it's really hard to claim back. So, you've got to make sure that they have the right rules and governance in place within the individual payment systems. But when you mix it with the gen AI components that you've talked about as well as what we see with data breaches and the manipulation and the education that are going on within social media, it just makes for a very dangerous cocktail. All those forces coming together where data is more available and accessible, as well as these powerful technology tools, it's just creating a very threatening environment. And so, we tend to believe that we need to start focusing our time on what some of those solutions can be.

David Jones [00:14:42] That helps, I think, lay the foundation for us in terms of what we're seeing on that risk level. As we think about the innovation being brought to this arena, right, with the type of impacts we highlighted at the outset of this conversation, billions of dollars both for businesses and consumers being put at risk and moved, how should we be thinking about some of the innovation that's being brought the bear in this arena? David, would you like to start on that topic for us?

David DeLeon [00:15:10] I'm happy to. And really the key here around effective fraud prevention is this concept around a multi-layered approach. So, it's not one silver bullet solution, but really a combination of solutions across people, process, technology, and data dimensions coming together to address the holistic risk factors that fraudsters are exploiting. So, this includes not just the monitoring of payments, but also things like robust onboarding processes and identity verification. Steven mentioned earlier around synthetic IDs and application fraud. It's looking at things like authentication and behavioral biometrics. So, there's some solutions on the scene now that we'll even look at. Have the angle of which you're holding your phone, or out of your fingers, touch the screen on your device to get more data to determine, is it really you that's conducting those transactions? Then even non-low tech type solutions like customer and employee education, educating customers around the latest scams, as well as employees on things like business email compromise that Steven had mentioned before. One of the interesting things we've seen, looking at the kind of customer education, there's oftentimes this conception that that's just the older generation that's falling victim to fraud and scams. But what we actually see out there in reality is, you know, the younger generations are also even more affected by many of the fraud schemes that are there.

So, it just brings to light the importance as well of combining technical solutions and more advanced, uh, analytical and AI solutions with, you know, the other components as well around education people in process to bring up a holistic solution together

David Jones [00:17:02] As we think about some of the activities specific to JP Morgan, Steven, if you wouldn't mind, could you take us further down the road of innovation and what you're doing for your clients?

Steven Bufferd [00:17:14] Sure. Thanks, David. There's probably two that I'd like to focus on today. One is around the use of a validation or a validation service. Validation service really is when you become suspicious, or you want to confirm that the beneficiary that you're paying is really who they say they are. Their names match, their account details look like they're legitimate. And so, we have a service called an account validation service that allows us to go out and very quickly confirm whether the account is open, the name on the account, meaning the beneficior of who you're paying, whether that matches. And we can provide you with that information before that payment is released. And clearly if there's anything or any of those signals that provide or create some suspicion you have the opportunity again to reach out directly and understand whether you're in fact paying the beneficiary you think you are paying. It's particularly good for when you're onboarding a new client or a new relationship or a new beneficiary. It's good when you receive an instruction that says that the beneficior has changed their um account details. So, it's a way of putting an extra check in the process for you before making the payment. The second service that I would point to as I talked earlier about the use of data and information and transaction history is actually the generation of confidence scores, where because of our scale and size, we're able to give an indication about what our prior history has been through a confidence core. That confidence core gives you an added layer of protection before releasing a payment that this is JPMorgan's payment history for its broad breadth of customers, they use us for payment processing services.

So, in a sense, when you bring those services together, is the account open, is that account in the right person's name, along with maybe an entity validation around whether that entity is real and not synthetic, along with a confidence score, it gives you a level of confidence before you're actually releasing the payment to the end recipient.

David Jones [00:19:3’] Steven, thank you for sharing how JPMorgan is thinking about innovation for its corporate clients. If you were to put on your merchant hat as an intermediary in this process, how should we think about some of the innovation and what the merchants, if you will, are thinking about specifically?

Steven Bufferd [00:19:46] You know, David, I think there's a couple of principles that they need to keep in mind. First and most importantly is the awareness, the training, and the testing that needs to go on within your own organization. Those individuals who are on the front lines, who are processing payments, who have to be suspicious and aware about cyber and fraud threats, that awareness and training is invaluable. We also think it's vitally important that within our own organizations, right, that we're evaluating, we're experimenting with new technology and some of the tools that are in place, that's both some of the services that we offer, but also activities that are going on within the marketplace. And I think each organization has their own risk parameters that they feel comfortable as they introduce new technologies but identifying the appropriate use cases. sampling it, testing, looking at your results and then expanding those use cases and the deployment of those tools is something that we would highly recommend. And lastly, it shouldn't really be overlooked, but it's also making sure that you have the right policies in place because the policies can drive what procedures and what practices get set up across the organization. So again, those three things that are important are the awareness, training and testing, really around the human element. It's evaluating and experimenting with new technology and tools. And then lastly, it's really around establishing the right policies and procedures and governance practices within the organization itself.

David Jones [00:21:25] Okay, David, we've had a number of points specific to digital payments. If we broaden that and think a little bit about checks, which is still a major currency, how would you suggest we think about the threats and solutions that are in that space specifically?

David DeLeon [00:21:40] Yeah, it's a good point, David. And you know what, what's really interesting is coming on the backside of COVID, what we ended up seeing in the industry was a resurgence of what we thought was kind of old school fraud around checks. There was some recent material that came out from American Bankers Association in January of this year that said 60% of all attempted fraud against bank deposits was made up of check fraud. So, a staggering amount. And what's actually happening is really a number of different schemes that fraudsters are using to either counterfeit checks, to steal and forge checks, even techniques such as, you know, washing and then kind of writing checks as if they're own. And so really what we're seeing is it's a big topic for a lot of financial services institutions currently and looking at a variety of techniques to then combat the risk of fraud and that can be everything from making sure that employees on the front line of banking centers are aware and are being vigilant for it. So back to education and process as well as technical solutions such as positive pay which has come out and been kind of directly targeted towards preventing check fraud by looking at check issuance verification of the checks and handling exceptions. There's also AI powered tools that analyze the check images and transaction patterns, so identify fraudulent activities and then even situations where SMS text messages are being sent to customers with check images to verify is this check yours or not before actually issuing the funds..

So, kind of a variety of techniques, again, not a silver bullet, but multiple. kind of tools and solutions being implemented to combat this type of threat.

David Jones [00:23:44] Okay so as we heard today this is an incredibly rapidly evolving area it's a complex problem it hits consumers corporates and merchants. As we think about some of our final thoughts for today, David, I'll start with you. Could you share how you're thinking about some other future points for our listeners to consider.

David DeLeon [00:24:02] Yeah, happy to. I think a few final takeaways, you know, one, unfortunately, fraud just it's not going away. It's only going to get more complex and sophisticated. So, it just has to be at the forefront and priority for financial services in the market today. Number two, is just continuing to invest in advanced technologies and solutions around this arena, you know, to fight the fraudsters, you really have to be playing a fair game and bringing the level of technical capability that they're using to effectively combat. And you know, it's going to take really the whole firm, if you think about the different components that we've, uh talked about here from education to process to governance, policies, controls, data and technology. It's a lot of parts of the that have to come together to help solve this. So, coordinating and doing this collectively across these organizations will be paramount. And then for the audience here focused on AI and innovation, it's an incredibly interesting time to be in this space. It's a unique opportunity to be part of the innovation. We're only at the beginning here of what is capable. And it really makes a huge impact within the financial services community. And then, for those of us that are using financial services products. So, it's an exciting place to be, in terms of anti-fraud. And there's still a long way to go. And I'm looking forward to seeing how the whole industry as a whole evolves to make the task at hand.

David Jones [00:25:37] Thank you for that, David. Steven, we'll turn it over to you from JP Morgan's perspective. We welcome your thoughts specific to the commercial sector and how you think about safety you trust every day.

Steven Bufferd [00:25:47] Yeah, David, a few key practical takeaways I'd like to give to some of the listeners. One really is knowing who your trusted contacts are at, your vendors, your suppliers, or people you're making payments to so that you have a way to. ensure when you're in doubt or have some suspicion about their information that you have a way to contact them directly and confirm their information. Make sure that you have the right procedures and policies in place, particularly around holidays or light staffing periods of time with the right level of expertise and that the team feels empowered to make the decisions that they need to on a payment center going out the door. And then lastly, really to the point of some of the capabilities we have here, which is really validating and confirming the information that's through an account validation, an entity validation or even use of something like a confidence score that gives you safety and security before you are hitting release and sending payments out the door.

David Jones [00:26:54] Thank you for that, Steven. In closing, fraud will continue to evolve. It's a problem that we, as we highlighted today, don’t have a silver bullet answer. Given this, both AI and innovation will continue to be critical. A huge thank you to our guests, David and Steven, for an enlightening discussion. See you next time.