M&T Bank
Managing Payments Risk During the New Reality of COVID-19

November 17, 2020
1 pm ET

V2 Producer Aaron: Ladies and gentlemen, it's my pleasure to welcome you to today's M&T Bank event, Managing Payments Risk During the New Reality of COVID-19. Before we get started today, I'd like to point out some of the ways that you can participate on today's event. And today's console, today's presentation utilizes a dynamic console that allows you to adjust and resize any of the windows available to you. You can drag them around or you can resize them by clicking on the lower right-hand portion of the window you wish to resize to change that to your preference. Also during today, we are going to be showing you a couple of polling questions and those will appear in your slides window. We do appreciate and encourage your participation in voting on those polling questions. You'll see those in the slide window and you'll click on the radio button that best corresponds to your answer. Make sure you hit the submit button that is going to be in the slides window to register your vote. Thanks again in advance for participating on those. We of course also encourage you to get the most out of today's presentation by asking any questions that you may have. You can do that by typing your questions into the Q&A window that you should see on the lower left-hand portion. Make sure you hit the submit button when you're asking a question and that will get the question into the queue. We'll take as many as we have time for at the conclusion of today. Lastly, before you leave today, we're going to be showing you a survey, so make sure to stick around for that. And at the very bottom, you should also see a green resource list button that has a lot of PDF information in there that's going to definitely be something you're going to want to look at it. And then finally, if you need any technical assistance on today, please enter a Q&A related question through that Q&A window I mentioned stating your technical issue. We'll be more than happy to help resolve any issues that you might be experiencing.

With that, let's go ahead and begin today's M&T Bank event, Managing Payments Risk During the New Reality of COVID-19. It's my pleasure to turn today's call over to our moderator for today, and that is Frank Lago, Group Manager, Treasury Sales with M&T Bank. Frank, with that, I'll turn it over to you.

Frank Lago: Thanks very much, Aaron. I'd like to extend my welcome to all of you joining us today. I'm Frank Lago, Business Lines Sales Manager for Commercial Payments at M&T Bank and your host today. This is the second of a series of online events to discuss topics in the Payment space that M&T is planning to hold. The first two events, we've been focusing primarily on the changing payments landscape as a result of the COVID pandemic, and more specifically, how the pandemic has accelerated current payment fraud.

One housekeeping note, we are pleased that today's program is approved for up to 1.2 CTP recertification credits by the Association of Financial Professionals.

You can find a confirmation of attendance form with the event resources at the bottom of your screen. Please retain a copy for your records in the event that you're audited.

During our earlier session, we provided a big picture view of the current environment for fraud and the additional vulnerabilities remote work has brought to the forefront. We received very good feedback from that event and hope that we provided information that has allowed businesses to shore up their defenses against fraud. Today we're going to focus our discussion more narrowly. We'll discuss card payments, both from the perspective of the card issuers and the merchant acquirors. One consequence of the pandemic has been faster push away from manual paper-based payments to more online electronic payments. Payments were trending in that direction before the pandemic and we see no reason to believe that there will be a reversal once the pandemic has run its course.

We're very fortunate today to have with us Kolin Whitley. Kolin comes to us as a Senior Director within North American Risk Organization at Visa, advising the top 25 issuers in the areas of fraud and identity management. Prior to joining Visa, Kolin spent more than 25 years in a variety of leadership roles for the payments and financial services in the public sector. Kolin is an internationally recognized subject matter expect in the fields of fraud and identity management and brings a wealth of industry knowledge having worked for a variety of top branded organizations in the payment ecosystem. As Aaron mentioned, we'll conduct a series of live polls as we move through Kolin's presentation and encourage you to submit questions in the Q&A box as we go through. To the extent possible, we'll answer questions during the presentation and Kolin will allow time at the end for a full Q&A. We'll also provide a survey at the end of today's session which we encourage you to complete. Your feedback will help us develop content for future events. With that, I'm going to turn it over to Kolin. Kolin, welcome and thanks for joining us today to share your expertise.

Kolin Whitley: Thanks, Frank. And thanks, everyone. I really appreciate the opportunity to be here and present on this topic. I don't think in the past 25 years of my career I've had to present on something related to a pandemic. So this is kind of new for all of us. I hate overusing the term "the new norm" but it is kind of is almost anything but at this point. I appreciate the opportunity to talk about this.

So this presentation I'm going to go through is really how we and our customers have responded to COVID-19. As we know, this sort of came on pretty rapidly. So a number of stakeholders were spinning and trying to react to this as quickly as they could. So within the North American Risk Team, our mission was to really leverage security as a catalyst for growth. One of the ways we do this is, in a perfect scenario, we try to decrease fraud rates, increase authorization rates and streamline the customer experience. Of course, that's our overall mission and goal. It doesn't always go that way and especially with something like COVID-19 sort of inserting itself into what we see as a normal payment pattern, this is what we're trying our best to do.

Within North American risk itself, we really look at this from a customer lifecycle approach. So everything we do, we look at right from the beginning where we look at account onboarding and management. So we use a lot of identity and analytics tools to try to prove that that person is who they claim to be before they even book an account. And then we look at the consumer identity and authentication, so making sure that the ongoing interaction between the cardholder, a merchant, and throughout the whole payment ecosystem is locked into that consumer's identity. That we're not seeing fraudsters take over that identity or other means of attack.

Then we also use a lot of analytics to look at transaction authorization. So every single transaction that goes through the Visa network is scored. We apply a score and we actually analyze the likelihood of that transaction being fraud. Being able to return those results to our issuing banks or acquirors in some cases, and even to the merchants three different programs to give them a sense that whether this transaction appears to be high risk or not. Then if it does, for whatever reason, become a fraudulent transaction, we look at supporting the dispute management process both for issuers, for the merchants, and the cardholder to make it as seamless as possible.

The underlying part behind all of this is looking at performance optimization. For those first four stages of the customer lifecycle, how can we ensure that the performance has been optimized to make the most easiest path for all of the key stakeholders. And when you look at the bottom of that slide, really what we're doing is, one of our pillars of security is trying to safeguard sensitive data. Leverage data for enhanced decisioning and I'll get into a little bit more of this further in the presentation of how we use artificial intelligence and other techniques to safeguard and enhance our decisioning process. And then how we deploy cybersecurity services. We have one of the most powerful cybersecurity groups in the world and I can explain what some of the great things that they're doing to help protect all of the Visa stakeholders throughout the Visa network.

So early on, I guess early on this year when COVID started to become quite a rapid reality for all of us, we had a lot of issuers and merchants and acquirors come to us and say, what should we be doing? What should we be looking for? Are there things that we should be preparing in order to deal with this new reality? One of the things that we did within North America is we created a risk health checklist. What you're looking at here is just sort of the summary of the different recommendations or different categories that we were looking at in order to determine what issuers, acquirors and merchants should be doing.

We really broke it down in to operational best practices of risk practices. Maintaining data security, as you can imagine, especially for a lot of issuers with working from home considerations, making sure that those issuers were adhering to the PCI compliance standards, safeguarding data, making sure that the employees that are working from home are taking -- doing what they're supposed to be doing and safeguarding the data that they're using day to day.

We also recognized that the fraud rules, there was no normal anymore. Historically, we had trends built in, or at least benchmarks built in to our fraud rules to look at velocity tracking, to look at the type of payments, whether it's card present, card not present, the merchant category codes that were coming through, which ones were high risk, which ones were not. When COVID came, all of that went out the window. We really had no bench line to work from. So we had to react almost in real time to adjust to the new environment of that shift in payment from card present to card not present. Even MCCs or different merchant category codes that would normally be selling products or clothing, were now selling personal protection equipment. Some of that caused a lot of spike in some of their transaction volumes. So being able to adjust to that activity on the fly was something that we worked with a lot of our issuers to be able to do.

Cyber awareness became really a key point, too. We saw a huge increase in cyberattacks with the onset of COVID-19. I think a lot of this was largely due to the fact that fraudsters knew that a lot of banks had people working from home, they didn't have the same structures in place to deal with cyberattacks, or even some of the resources, access to the resources to deal with cyberattacks if they came in. We saw a huge increase of that, a lot of it coming from foreign actors. We saw a lot of attacks coming out of North Korea, we saw attacks coming out of China. We also saw a lot of attacks coming out of Latin America. So as I mentioned before, we have a cyber security team that looks at this stuff at a network level and is able to respond quickly. It did force us to create a few new tools in our toolbox to be able to deal with these types of attacks as we detected them.

There's also the government regulatory considerations. There was a lot of stuff that we knew that was going to come out early on as far as stimulus payments, people filing for unemployment insurance. And we started seeing a huge amount of fraud associated with that, where a fraudster would steal someone's identity, apply for unemployment insurance on their behalf, get that prepaid card, monetize it, cash it out, then dispute the transaction with the issuing bank and do it again. So a lot of double-dipping going on with fraudsters. We've seen some banks within the US got hit with at least $800 million in this type of fraud. So it's something that is not going away any time soon. We're working very closely with the issuers, we're working with the state agencies that disburse these prepaid cards. Because as you can imagine, prior to COVID, the amount of volume they were seeing made it much easier for them to validate things like identity of applicants and things like that. With the new regulatory policies in place, they have I think up to 2 days to make an assertion of that person's eligibility for those payments.

So with millions and millions of applications coming through, they just don't have the tools or the know-how to properly identity-proof someone before issuing those cards. So again, all of these things were stuff that was basically brand new to the industry. We've been able to try to react to it as fast as we can while also being somewhat proactive to try to prevent this type of stuff from happening again.

So again, looking at addressing the new normal. And again, this changes all the time with our issuing banks. We're constantly talking to them about some of the changes we're seeing. Changes in business operations. Again, as I mentioned before, working from home, how do you make sure that you're safeguarding the data and then deploying cybersecurity to make sure that you're securing the network and the payment system.

Some of the early observations we saw, certainly at a global level, we saw a year over year decrease in total authorization requests and approvals. So a lot of this was again related to just lack of volume, number one. A lot of people were either sheltering in place, they weren't spending like they normally would spend. And people were just sort of on hold. So we saw a definite decline in that. But we also saw a lot of declines increasing, too. Because of the activity being abnormal and not like it was pre-COVID, a lot of issuing banks were declining perfectly good transactions for fear of fraud. So we also saw a massive migration from card present to card not present. And for obvious reasons. People were just not wanting to go out and buy face to face in stores. They were starting to buy stuff online. So we saw a lot of card not present volume increase. But we also saw a fraud associated with that as well. As you can imagine, with card not present, you don't have the same types of controls you do in a card present environment. You don't have a chip card, you don't have that EMV protection. You're relying on scoring models to try to pick up unusual behavior.

Specific to North America, we saw sales decline pretty rapidly as well. It was mostly in that travel and entertainment sector with airlines, lodging, restaurants. They were all the most impacted. And again, for some obvious reasons. People just stopped traveling. They weren't traveling, they weren't going out to restaurants. After the initial spike in sales due to panic ordering, we saw the toilet paper purchases I think everyone is aware of, and people buying personal protection equipment, masks, gloves, all of that stuff. We saw a rapid rise in those types of sales. But as that started to kind of taper off, we've seen now fraud moving to -- the primaries had declined slightly in the card present segment, but then as I mentioned before, they rapidly increased in the card not present.

We also saw an increase in global disputes. These were chargebacks or disputes from cardholders. Some of this we saw was related to what we call friendly fraud or first party misuse where a cardholder might have purchased something online or they might have been playing a game online and they lost, so they dispute the transaction and say it wasn't them in the first place. Or in some cases, it was related to travel and entertainment, too. Some people had booked travel plans and due to refund policies with that merchant, they may not have been able to get a refund. So they would go ahead and dispute the transaction with their issuer to try to get their money back. So a lot of different observations early on. We're continuing to see it now, but it's starting to somewhat normalize a bit. We're starting to see more normal activity than certainly we saw back in the early spring.

We were also looking at this from a merchant perspective when we had a lot of acquirors come to us saying, you know, we know what issuers are doing. We know they have some controls in place. How do we provide best practices to the merchant segment? So we pulled together this BOPIS plan we called it, which is really Buying Online, Pickup In Store. This sort of began the new norm where people were just buying, so they were using a card not present transaction to buy products online and then they would go pick it up in the store. So we pulled together these best practices to try to educate some of those merchants that really hadn't dealt with that type of transaction before, some of the things that they could do to try to protect themselves.

The following online purchase controls like implementing and actively maintaining ecommerce broad management solution, employee manual review process for high risk or high dollar transactions. We gave a number of best practices throughout here to just try to give them an idea of what are some of the easy things they can do to try to either detect fraud or prevent themselves from being a victim of fraud. Some of these things, too, required them to build their own transaction fraud rules. Looking at device profiling technology, that became really popular for a lot of the larger digital merchants where they would be able to actually look at the device intelligence or the device details with that computer that is interacting with them to identify certain risk elements within that that might give them an indication of fraud. It can either be that device was associated with a fraudulent transaction in the past with them, it could indicate that the IP address that doesn't seem to match the address they're wanting to have these goods shipped to or where they're coming from. So there's a lot of things, a lot of solutions out there in the market that merchants started to track or just started to utilize in order to track this type of fraud.

Some other recommendations we provided too, dealt with pickup controls. How to train staff to really handle secure transactions when they're doing things like curbside pickups, asking for identification at the time of pickup. We realize this isn't something that you can do for every transaction, but if it's a high-risk transaction and this person just bought a television and they're picking it up curbside, you probably want to do something to verify that that person is the card holder that purchased that item online. Looking at even providing apps or mobile browser-driven customer tools. We've seen a lot of restaurants do this early into COVID where you could download their app and you could use that to purchase things. What that did was it actually gave the merchant a lot more security in knowing that that app is on that mobile device that has been interacting with them and that mobile device belongs to the person that is making the transaction. So those became very powerful tools that a lot of our merchants were starting to use.

Even on some loss prevention teams, assess pickup locations for CCTV surveillance, like putting cameras outside the store if you're doing curbside pickup. So at least you would have some sort of history or information that could be used with law enforcement if in fact the transaction ends up being fraudulent. Audit, inspect parcels awaiting pickup. Consider controlled access to storage area containing fulfilled orders waiting for pickup. We heard some really nightmare stories of some especially electronics stores where they would stage merchandise that was ready to be picked up near the door knowing that someone was going to pull up any minute now and pick up their stereo system or their new TV or their laptop, and then fraudsters would just walk in the door, grab them all at once and just run out the door. So some of the things that we just wouldn't have expected historically became kind of the new norm.

So Frank, it looks like we have our first polling question.

Frank Lago: Yeah. So at this time we're going to go ahead and have you please respond to this poll. The question there, has your company been the target of payment fraud since the pandemic hit? Kolin, while we're waiting for those poll results to come in, let me ask you a question. Commercial cards were relatively rare 10 or 15 years ago. Today they're quite common. Have the fraudsters moved to target the commercial side of transactions more than retail personal cards? Or they simply expand their universe of potential victims?

Kolin Whitley: I think it's a bit of both. They certainly have targeted the commercial sector. I think one of the reasons that they have done this is that commercial transactions tend to be larger in size. It's not unnormal to have big ticket transactions come through that with a normal consumer card might look risky or abnormal. In a commercial setting, it doesn't. So it's much easier for them to hide fraudulent transactions, still monetize a significant amount of money before setting off any alarms. That said, we also see in some cases that fraudsters have a much shorter run on commercial cards than consumer. one of the reasons for that, you typically have program managers or people that are looking at the transactions and scrutinizing them for their own internal audit purposes. So they usually catch that stuff much more quickly than a consumer would when they're waiting for their statement at the end of the month and they might or may not notice an unusual transaction.

But we also have seen I kind of call it the squeezing the balloon effect. Fraud always pursues the path of least resistance. So if you're a commercial issuer and you don't have the same types of controls in place or fraud rules that you would on the consumer side, you know, fraudsters will definitely exploit that. And they'll also exploit other mechanisms too, like identity takeover and account takeover of commercial cards, things like that where once they get ahold of the actual card themselves, then they'll bust it out as quickly as they can and monetize as much as they can within that short amount of time.

Frank Lago: I know we've got a lot of card program managers on the call today. I'm sure they appreciate that additional insight. Why don't we go ahead and look at the poll results, Kolin, if you want to advance the slide there?

Kolin Whitley: Sure.

Frank Lago: So the good news here I suppose is that about 70%, almost 70%, 68.2% of the attendees who responded today said they have not been subject to fraud. But I've got to say that almost 32% of you have been the target of payment fraud is not really surprising, but it's certainly a little bit disturbing. Thanks, everyone, for participating in that poll. We're going to have another question coming up in just a few more slides. But, Kolin, why don't you go ahead and pick back up here?

Kolin Whitley: Sounds good. I wanted to spend a little time talking about internet of things or IoT as we refer to it as. Some of you might remember back in the late 90s there was that old adage, on the internet, nobody knows you're a dog. People probably saw that little cartoon. We advanced to 2021 and now online, nobody knows you're a refrigerator. So we've seen a change in technology over the past decade especially where things have been enabled on the internet that previously we wouldn't have even imagine. I don't think any of us really 10 years ago would have imagined a refrigerator, ordering groceries through your refrigerator on the refrigerator door. And having wearables that can be used for payments such as Apple watches, and even vehicles now are becoming more connected to the internet, whether it's through app systems, whether it's through using your car play functionality through your iPhone, or what have you. There's so many examples now where devices have been connected to the internet.

The interesting thing to note, too, is that when you look at the value of IoT payments, 70% of retailers are ready to adopt IoT. Even when we look at it now, the value IoT payments is expected to reach $410 billion by 2023. That is a massive increase and looking at an annual rate of 75% plus from 2018 on. So it's something that is growing rapidly, but with that obviously, comes a lot of problems. When you think about all of the safeguards you might put in place with your laptop, you might have an antivirus program running or you might have a VPN that you're working with, or any of those controls that you can typically put on a normal device that you would interact with on the internet. But these devices, they just don't have the same controls. So if people are using them appropriately, then you would probably want to use something like a VPN at your router level or something to that effect. But even then, you can't escape when you're outside of your home or you're in the wild using devices to interact with people. So it's something that fraudsters are really starting to exploit now.

We did see an attack even recently, this was one of the attacks out of North Korea. They were using a piece of code called Lazarus that would actually be used at an ATM level where they would circumvent the controls of an ATM and effectively turn off all controls and have these ATM cash attacks. They would orchestrate these across a large geographical area and they'd have a few hundred people involved in this all standing in front of an ATM and they would flip the switch all at the same time and empty the cash machine all in one shot. They did it all at the same time so that issuer banks didn't detect it until it was too late. They just had no possible way of preventing it. So we're seeing these attacks. We haven't seen it in North America yet fortunately, but we have no doubt that these types of deployed attacks exploiting IoT devices is something that will continue and probably be here before too long.

So when we look at IoT commerce, it comes with its own set of security concerns. As I mentioned before, we're seeing these new attacks coming out all the time. What I noticed here in the first half of 2020, there were 2.9 billion IoT related network attacks. These are things that we monitor for, at the Visa network level. We have an operations center called the ROC or the Risk Operations Center within the US that is kind of a bunker that looks at monitoring the Visa net activity 24/7. What they're looking for is anything that might indicate an abnormality in payment traffic all around the world. It's a pretty powerful set of controls that we have when you think of the Visa network and the billions of transactions that are performed all the time around the globe. We're able to detect specific attacks in the system and react to them very quickly. We've actually built some controls that allow us to block at the merchant level, so the issuer never even sees that traffic coming through because we detected it at the network before it even hit the bank.

But some of the areas that when you're looking at building your own controls around security around IoT, you want to look at things like device security. You want to look at things like data privacy that you're not collecting more information than what you need, and then you're looking at your network security. So this is again, you're pen testing, working with organizations that can test your network. While we might be secure on our end, if your network is not secure itself, we've seen a lot of attacks that way. We've seen a real increase especially during COVID. I don't know if the folks on the call have seen this as much as I have, but I would say at least three times a week I get a text message saying, hey, you just won your new laptop or you won this or you won that. Click on this link. Those are all typically a form of phishing attack. We call those, because it's an SMS, we call them smishing attacks, but they're all the same thing. They're trying to get you to click on a link so that malware can be deployed on your device without you knowing and then your device is exploited to make unauthorized payments on your behalf. So again, it's something that we're tracking closely, but when you are looking at your own network security controls, always make sure your patches are up to date, always make sure that you're constantly looking at any vulnerabilities that might be in your system.

One of the interesting evolutions we've seen too over the last several years is this whole concept of digital identity. When we say digital identity, it's really the binding of an identity credential to who that person is. When you think of it, you've probably seen these things where you signed up for a website and they'll say do you want to log in with your Facebook credentials or your Google credentials or Microsoft? All of those things are great from a convenience perspective, but they're not remotely secure. When you think about when you open a Facebook account, anyone can do it, they don't really do anything in terms of verifying your identity. So once you have that Facebook credential, if you're using that to log in to something that might expose sensitive material, it's something that you obviously just don't want to do, right? I've told so many people, whether it's family and friends, never use those types of mechanisms to log into sites. That being said, there is a future when we look at real identity down to a physical identity or a digital identity, those are becoming much more popular. That's some of the innovations that we're working on at Visa as well, is how do we assign a credential to a person that can be trusted so that they can use that credential to log into multiple endpoints? One of the main reasons for this, well, there's two main reasons for this. One is to create a seamless experience for a card holder so you're not having to come up with a user ID and password for umpteen different sites and try to remember what those are and all of those things. But also to make it more secure. Because passwords can be intercepted. I get messages all the time, if you sign up for an identity service, saying, hey, we found your password being sold on the dark web. You might want to change it. Things like that happen all the time. But with a digital identity, it makes it virtually impossible to crack. Because you're effectively tokenizing yourself as an identity. Once that's bound, it's difficult to unbind that.

That said, it's only as good as the person that created it. If you have a fraudster creating a digital identity and all you're doing is verifying that, yep, that's still the fraudster, it's not going to help you out much. So the enrollment process when you look at these types of technology are as important as the solution itself. Again, it's more of just things to come that you're going to start seeing a lot more talked about in the coming years is this whole concept of digital identity.

One of the things we've been working on for quite some time too is biometrics. And I think everyone has been exposed to biometrics at this point in their lives, whether it's opening your iPhone, whether it's using a fingerprint reader, all of those things, it's increasing rapidly. We expect it to increase even more rapidly as we move forward. One of the reasons for this is kind of what I showed in the previous slide, it's just that whole idea of a convenience of security. Biometrics is something that I think the US was probably late to adopt. I think a lot of Americans were just not comfortable with that or giving up a piece of their biometric that might be stored somewhere and that might be hacked or someone might steal it. So there was a lot of pushback I'd say earlier on. Ironically, I think once they could show that biometrics made things more convenient for cardholders, we found that 9 times out of 10 convenience will trump security every time. Cardholders would be much, much more willing to give up that biometric if it means they don't have to type in a password each time they want to open their phone. So we're seeing an increase in this and we see it as kind of a sign of things to come especially when you can combine or you bind a biometric to that person's digital identity, then it becomes even more secure. So we're starting to see more use cases for this that are growing. But the one caution I will give on this as well, is it's still only as good as the enrollment. So if you're enrolling a fraudster's biometric or thumb print, you can't unbind a biometric. So once you've bound that to that identity, all you're doing is verifying that that is the fraudster moving forward. So again, if you're utilizing this type of technology, you need to make sure that the enrollment process is secure and as thorough as you can possibly make it. Because that's the one attribute that you're going to be trusting for the rest of that person's relationship with your bank or your cardholder.

So, Frank, it looks like we've got another polling question.

Frank Lago: Yeah. Time for poll question number 2. So this time, the question, you can see it there again, has your company taken any additional steps to protect against fraud since the pandemic hit? I certainly hope that the 32% of individuals who've experienced some fraud have now at least taken some additional steps. I'll go ahead and allow a minute for answers to come up there.

And Kolin, let me circle back for a second on the Internet of Things. I think it's another situation where technology is here to make our lives easier, but the consumer of the technology doesn't understand it so well or doesn't understand the vulnerabilities it creates. You had a number of suggestions there, but if you could just make one suggestion to folks that help prevent intrusion for someone who wants to add their garage door opener, their refrigerator, their thermostat to their home network, what would that one piece of advice you give them to kind of protect themselves there?

Kolin Whitley: I think the best advice would be to use technologies like VPNs within your home. They're becoming a lot more popular now. I just set up my son's computer just yesterday. He got a new computer and we set it up and I assigned it to a VPN so I knew he would be protected. You know, kids are sometimes not the greatest at picking up on phishing e-mails and things like that. So using some sort of control at your network level is best, I would say. You know, not to knock technology, but be careful of the things that you do assign access to your network. They might seem like they're really convenient to do that but just make sure that if it's assigned to your network, that it does fall under that protection of something like a VPN.

Frank Lago: Yeah. great advice. Thanks. So let's go ahead and take a look at the results. Then we can move into the final part of the presentation here. 62% have said that they have taken some steps, so again, it's good to see that folks are very aware. Obviously, I would think this audience, having taken the time to participate this afternoon, is probably very aware of the threat out there, so it's good to so that many of you are taking the advice to protect their businesses a little bit better. So 16.1% aren't sure. I guess that's just because of the role that you play. But again, I think a healthy number of folks here taking the right step. So Kolin, let's jump in to the last section of the presentation here.

Kolin Whitley: Sounds great. Thanks, Frank. So this next section here, I want to talk a little bit about increases in identity fraud. This is something that we've seen a real surge in since the onset of COVID. As I mentioned earlier in the presentation, what we saw taking place during almost immediately after the stimulus payments went out was a number of fraudsters that were taking over a real person's account. They were taking -- basically, accessing their identity that they would either buy on the dark web, that fraudsters are buying and selling this information from prior data breaches, or they would commit something that we call social engineering where they would contact the cardholder and say hey, this is your bank calling, we've noticed some unusual transactions. Can you verify your identity for us before we can go any further? Some cardholders would tell them everything, their name, address, date of birth, social security number, everything that that fraudster needs to now call the actual bank and take over that account.

We also saw an uptick in e-mail accounts being compromised where people have weak passwords for e-mails. Once they could attack that e-mail, they would look for any communications from a bank that might e-mail that true cardholder and then they would go to that bank and click on -- they would know a lot of people use their e-mail address as their user ID, they would take an attempt at that and then click forgot my password. So what does the bank do? They send them a reset request through email. And so the fraudster then compromises that and they go to town. There's so many different ways that this has been taking place. But what we saw on the monetization side has really been around this unemployment insurance fraud scheme. Where they would again use that personal information to apply for unemployment insurance, go to that state agency, pick up their prepaid card or that card would be mailed to them, and then they would use it to make fraudulent purchases. Usually in collusion in some cases with a fraudulent merchant. And then in the first case, it's obviously the state agency is out the money. But then when they dispute the transaction with the bank and that bank replenishes those funds and they do it a second time, the bank is out that money. So there's double-dipping attacks we've seen. And as I mentioned before, we've seen banks lose over $800 million just so far as a direct result of that unemployment insurance attack.

So it's something that we're seeing growing quite rapidly. From an advice perspective, I would say some of the things that you can do to protect yourself from this is, never accept an unsolicited call from a bank asking you to verify your identity. It likely will never happen legitimately. And if you are ever suspicious, hang up the phone, turn over the back of your card, call that number on the back of your card to your actual bank and try to verify that communication.

The other thing you should be doing, too, coming from somebody working for a credit bureau at one point in time, check your credit report pretty constantly. I would suggest checking it at least 3 times a year just to look for any changes. Is there any new trade lines that have been posted that you're not aware of? Things like that just give you another sense of security that you're not a victim of this ATO attack.

Artificial intelligence is something that you're probably hearing a lot more about as well. At Visa, we've been using artificial intelligence for quite a few years. We're probably one of the first companies to use it in order to look at transaction scoring. We use it to train for automated machine learning. We have artificial intelligence-enabled chips. We also utilize natural language processing. And all the while, there's more capabilities being built all the time. So something that is sometimes scary to some folks when you think of -- you start thinking of machines taking over the world through artificial intelligence. But trust me when I say, we're using it in a very safe and secure way and it's given us the ability to really learn how fraud patterns are being developed in real time and being able to react to them to protect our stakeholders before anyone even realizes what's going on.

So as AI creates more convenience for consumers, it obviously posts some security threats as well and some of these I've mentioned before around phishing attacks. We've seen a lot of increase in that. Behavioral detection. It's being used to observe patterns of normal user behavior and then mimicking those so it can look and see how you normally transact, whether it's in person, online, and then mimic that activity so that the bank won't detect it as being unusual, but then a fraud still being created. As we shift a lot of things to the cloud, that's also become a big vector for attacks. We see that there's mass amounts of information being stored on the cloud these days. So obviously it's going to be a target for us for using AI to infiltrate those storage facilities.

We also see vulnerability discovery in software. We've seen in some cases that computer manufacturers, we've even seen computers being shipped from China that have malware already within the device itself that is being used to pick up information from the end user's computer once they activate it. So we've seen stuff like that. We've also seen AI being used to find those vulnerabilities within that device and exploit them by learning how that device actually works. So again, there's a lot of stuff that you can probably speak all day on, on artificial intelligence, but it's something that has become much more highly used from a fraud prevention perspective but also used as an attack vector during COVID-19.

During the second half of 2018, we saw more than 2.1 billion bot attacks targeting ecommerce sites. And this is something that I used to work for an organization that created bots that would go out on the internet, on the dark web, and look to see where people were buying and selling stolen identity information and we'd scrape that information from those sites and notify the actual owners of it to help them protect their identity. This is something that has been around for a while, but we're seeing these bots being attacked in the ecommerce merchants especially, looking for vulnerabilities within that, their merchant platform. We saw a lot of card testing activity taking place over the last several months during COVID where we call them numeration attacks where they would run through hundreds of millions of bins through a merchant that didn't have and sort of controls in place to prevent it. And in order to try to find a bin that worked that they could then exploit. So we've seen a lot of these and in some cases, we -- in one situation, we saw several golf merchants that were being attacked. We couldn't figure out why someone would be attacking a golf merchant until we realized that the developer of the website for that golf merchant was the same on each one of those golf companies that got attacked. So the fraudster has obviously identified software that was being used that had a vulnerability and they were using that as the attack vector to test cards. So what we do in those cases, we usually recommend to merchants that they put in something as simple as CAPTCHA on their website to stop these bot attacks so that they don't become a victim of this type of account testing.

So you hear a lot about mobile apps for NFC fraud. You know, those are those near field or tap to pay. We haven't seen much in terms of vulnerabilities with that. You hear a lot of stories on the news about oh, you know, someone stood behind me and they scanned the card in my wallet, I need to get an RFID wallet and all these things. I can tell you right now, that just doesn't happen. There has been a few isolated events where that has taken place, but they're always limited to low-dollar transactions anyway to begin with. And if they actually get a transaction to pass once, they can never do it a second time because it's a dynamic tokenization within NFC, kind of like a chip card that even if you compromise the chip in a card, you can only use it once because the keys change constantly. So just rest assured that this isn't something that we're seeing as a significant attack vector for fraud at this point. But we do know that tap to pay is becoming hugely popular especially because of COVID-19. Anytime that you can have a contactless transaction, you're going to want to do that. But you can do so knowing that it's secure.

So when we look at some of these enumeration attacks, some of these other attacks as I mentioned, it's a very complicated problem. The reason for that is it's global in nature. A lot of these enumeration attacks we've seen initially came out of Latin America. Specifically, Brazil, where we were seeing fraudsters just -- sometimes we call it card tumbling where they're just using multiple bins to try to get a transaction to work. And it usually involves multiple merchants, acquirors. The potential of impacting legitimate activity -- because what happens in many cases is that just due to the velocity of the attacks being made, a lot of the processors will time out, forcing the issuer to go into step. If they don't have the same security controls in step that they had in their normal fraud environment, fraudsters will exploit that and monetize those transactions. The good thing, it's a solvable problem. As I mentioned before, we have a risk operations center that looks at these transactions on a global level and can pick up on them using artificial intelligence and a number of other different tools in our belts to really detect it quickly and shut it down before any fraud actually takes place. The interesting thing is that we're one of the only networks that does that. We have this ability to -- this attack vector prevention capability that just uses artificial intelligence, again, to look for abnormal activity for certain merchants. It's not typical or previous of historical behavior and can shut that down in real time. So in many cases as I said before, the issuers don't even know it's happening. We just do it to prevent them from being a victim.

Some of the disrupting criminal operations, too. As I mentioned earlier, with some of these attacks coming out of North Korea, some of them coming out of Latin America, we do work with local law enforcement groups all the time. In the US, we largely work with US Secret Service and the FBI and we provide them with a lot of intelligence they need to take down these large organizations. One of the things that people don't think about a lot that is really disturbing is, banks may say okay, you know what, we lost $200 million this year in fraud, that's not too bad. That's kind of what we budgeted for. Well that $200 million goes into human trafficking, firearm sales, narcotics, terrorist financing. So we've worked with international law enforcement to take down a lot of these criminal groups around the globe. So it's not just the case of a basis point fraud loss, this is stuff that is being used for really bad, bad purposes. So we try to do the best we can to protect that side of the business also.

So how are we fighting back? I mentioned some of these before. We have a number of different tools at our disposal that we can utilize either next to or in real time. So our Visa account attack intelligence, real-time attack disruption, those are some of the things I mentioned around being able to block at the merchant level. Our Risk Operations Center, we have former NSA employees that work in our intelligence center that actually are monitoring a lot of this stuff 24/7. We also send out multiple acquiror and issuer notifications when we do see trends that are coming out. We do have a threat report that we send to all of our issuer clients that can tell them what are some of the new schemes we're seeing and how they can protect themselves from becoming victims.

Threat actor identification. This requires collaboration of course, but we work with a lot of our issuers, acquirors, and in some cases merchants as well, to try to coordinate investigations as they come through. And then law enforcement engagement. We have a lot of great police agencies that have worked with us to really help take down some of these massive crimes as they come through.

I think this is our last polling question, Frank.

Frank Lago: Yeah. So this time it's more of a multiple choice question for you rather than yes or no. So I'd ask everyone to take the time to complete the polling question and we'll start to get into our Q&A. As a result of what you heard here today, do you believe your company is well-protected against fraud, somewhat protected, or oh, boy, better talk to somebody about fraud prevention now? So go ahead and, Kolin, while we're waiting, we'll give a minute and I know we're going to move right into Q&A. But I'm getting a lot of good questions here. So let me just start to hit you with some from the audience if you don't mind. The first one here, what's your perspective on password managers? I fear that everything is in one place and if they hack into that, they would have all of my log-ins.

Kolin Whitley: It's a good question. I would say it's better than not using one in some senses, but be careful of the ones that you do use. Make sure if you're using a password manager that it's a very highly key-encrypted device that you're using. I use it sometimes myself because it does provide essentially uncrackable passwords that are next to uncrackable. But yeah, make sure that you're researching the password manager that you're going to use before you deploy it. Because they're not all at the same level of security.

But I would say it's definitely better than the typical method of certainly writing down your password on a sticky a note and putting it on your monitor. So if you can, avoid that. But it you're looking at just coming up with your own passwords, make sure that they are extensive. I usually try to recommend people, make your password a phrase. Something that only you would know. Or just make sure you're changing them rapidly, too. Because I would say even in the case of a password manager, I would still recommend that you change them fairly frequently. Because to the point of the question, if that ever does get hacked and they have all your passwords, if you're changing them relatively rapidly, they're still not going to be able to use them because they're going to have to keep doing it over and over again. But it's a good question.

Frank Lago: Great. Thanks. Why don't we go ahead and look at the results of our last poll here. And then I'll get you to answer some more questions. So just a little over half have said somewhat protected but have work to do. I think that is probably not a surprise to see that being the predominant answer here. I think we can always try to do a little bit more, right? But it's heartening to see that almost half, they are pretty well-protected. For those, Kolin, what do you say to those that think they're well-protected? Do you think -- I mean my inclination is that is great to see, but given the prevalence of fraud I know we see at M&T, and I can't even imagine the amount you guys are seeing in Visa. Do you think there's some false confidence here?

Kolin Whitley: It's quite possible. You know, I'm not going to necessarily argue against folks that say they have great controls. But I would say that even if you do believe that you are well-protected against fraud, look, look, look again. Make sure that you're constantly reviewing your policies and procedures. Look at your network controls. Look at anything that you can that might, if it did become vulnerable, could be devastating to your organization. In some cases, you know, Visa is happy to work with a number of our clients to help them test their networks. As I said, we've got a lot of talented people that we can perform that type of testing. These people basically act like they're fraudsters and try to exploit your network. And if they can get through, then they can at least show you what you need to patch up or what you need to fix in order to stay secure. My recommendation, again, is just keep reviewing it regularly to make sure that everything is up to date and that you are protected.

Frank Lago: Okay, great. Yeah, I was trying to be a little provocative there. So let's go to another question. We have about five more minutes to take some questions. Relating to financial account takeover fraud, banks utilize most for the restoration services after customers identify -- customer identity has been compromised. How about securing and monitoring these accounts? So I'm not sure if that is really your level of expertise, but you do deal with a lot of banks, Kolin, so do you have an answer for that of who banks are going to most often when there's a problem of compromise on their end?

Kolin Whitley: Yeah. There are a lot of great solutions in the market right now. I used to work for Experian and they bought a company called CS Identity that is also a company I used to work for that has that type of identity monitoring service. I think most of them work in a very similar way. But I would say even though deposit accounts and things like that don't deal with credit bureaus, some of the solutions that those credit bureaus provide to monitor identities, all work well. The one thing I would suggest though is, if you're trying to get a consumer to sign up for those types of services, make sure that you are using a service that doesn't send out too many alerts like false alerts. Because I find consumers can adopt this thing called alert fatigue where once they start seeing alerts every other day, they just stop paying attention to them. So make sure you're using a reputable service. There's a number of them out there that work quite well. Make sure that you are using it for a long period of time, because a lot of fraudsters, after a breach, know that customers are going to get these identity monitoring solutions, but they'll typically only have it for about 2 years before they stop using it. So they'll hold onto that identity for 2 years and then start monetizing it. So make sure it's consistent in its ongoing usage.

Frank Lago: Okay, great. Thanks. Here's a straightforward question. Debit versus credit cards. Is it safer to purchase online with a credit card or debit card?

Kolin Whitley: That's an easy one. It's your credit card. It's obviously much safer. The reason for that is, if you do suffer fraud on that card, you're not going to pay for it. It's not money out of your bank account like it would be in a debit situation. We've heard some pretty nightmare stories of debit cards being compromised and used fraudulently to drain a bank account and then the person's house insurance doesn't go through and they lose their insurance or things like that that are quite scary. So obviously Visa, MasterCard both have zero liability capability within their credit cards. Even for debit, but debit still takes a while to get the money back, where credit, they can at least -- they're required to by law replenish those funds as quickly as possible while they conduct an investigation so you're not out the money. So credit over debit online for sure.

Frank Lago: Great. The next one I think I have an answer for, too, but I'll let you take a crack at it as well. Does business cyber insurance help protect us should bank fraud occur? The M&T Bank has an insurance agency that provides cyber insurance. We certainly feel that that could be one of the tools to protect yourself should there be an occurrence of fraud. But just like with any insurance, it's not really a replacement for taking good care to put preventative measures in place in advance of that, right? It's got to be your fallback position. You should always have good fraud controls on your accounts and services. Anything to add to that, Kolin?

Kolin Whitley: No, I would agree with you completely. I guess the one thing to consider is, even with insurance, cyber insurance, it still doesn't replace the identity information that may have been stolen, right? That's not something you can get back, so once it's gone, it's gone. I agree with you, it's more of a fallback, but you should not rely on it as your safety net. It should be controls upfront so you never have to use it.

Frank Lago: Okay, we have a few more questions, but we're about out of time. Let me ask you one more and then I'll just tell, for those that have submitted questions that did not get answered, we will make every attempt to get back to you on your e-mail address and we'll e-mail you and answer directly. But, Kolin, last one here, for the backend of infrastructure, is there an existing use or future planned use of blockchain to enhance security?

Kolin Whitley: Yeah, we've certainly looked at blockchain. We've looked at a number of different technologies. It's difficult for us to rely on blockchain ourselves at this moment just given the amount of data that we have. I think as computing capabilities increase and we start getting into more quantum computing capabilities, the use of blockchain is going to be much more feasible. But just given the amount of data that we process today, it's very difficult for us to do that. But we are looking at it very closely and we're looking at other technologies as well that are sort of that ledger-based type of control.

Frank Lago: Okay, great. Well, Kolin, I'd like to thank you very much for coming on today and thank all of those who are attending. Please take the final survey as you'll see come up on your screen in just a moment. Remember that at the bottom of your screen, you should see a resources button. You can get a lot of the information that Kolin shared today, some good resources down there, as well as your CTP certification credits. But with that, we're going to go ahead and wrap it up and tanks again, Kolin, and thanks, everyone.

Kolin Whitley: Thank you.