ATM Attack Trends and Defenses Transcript - November 3, 2022

Federal Reserve Bank of Atlanta *Talk About Payments* Webinar

ATM Attack Trends and Defenses

June 9, 2022

Transcript

David Lott: ...content of the webinar, I'd like to cover some of the logistics associated with it. We certainly want the webinar to be informative and valuable for you, so we have the opportunity for you to ask a question during the presentations made by our expert panelists. Just simply, in the "Ask a Question" or Q&A box on the platform, enter your question and we will hold those questions till the end of the webinar and address as many as we can.

If you have any technical issues with regard to your connectivity, please use the chat box. Our production staff will be monitoring that and will try to assist. Thirdly, we have a survey being conducted at the end of the webinar that we would certainly ask for your participation in. It provides excellent feedback for us in terms of the value that we're providing in these webinars, as well as understanding what topics you would like us to address in the future.

This webinar is being recorded, and the recording of the webinar, the presentation deck, as well as a transcript of the presentations, will be made available generally within a week of that on our web page—you see the link to that.

Next slide please, David.

For those of us joining for the first time, let me quickly tell you a little bit about the work of the Retail Payments Risk Forum here at the Atlanta Fed. Our primary functions are research and education. On the research side, we do the triennial payments study—and just last week we released the 2021 Survey and Diary of Consumer Payment Choice, which is the only national survey that tracks cash usage by consumers. We hope that you will use those research documents in your work, especially those of you in the ATM field looking at the activity of cash over the last several years as impacted by the COVID pandemic.

The other aspect is education, such as the webinar that we're conducting right now. We do a weekly blog as well, on different payment issues. As a matter of fact, the blog this week discusses some of the changes in payments with regard to online payments in the food industries, both grocery as well as casual and fast-food dining, that you might find interesting. So again, we hope that you will use our web page as a resource for the future.

Next slide please, David.

As far as our agenda today, we're going to start off with introductions of our moderator and our expert panelists, who are going to cover these three areas: the attacks against personnel, both service personnel as well as cash-in-transit personnel. Then we'll look at the virtual attacks against the ATM channel, followed by the brute force attacks, the physical attacks, against the ATMs themselves, and looking at some of the activity and the trends that have taken place.

As I mentioned before, we're saving some time at the end to address the questions that you have. So again, feel free to add your questions as you listen to the content on any follow-up that you would like to have.

So, next slide please.

With that, I'm pleased to introduce David Tente, who will serve as the moderator for the webinar. David is the executive director of the ATM Industry Association as well as the executive director of the ATM Security Association. David will further introduce himself, as well as each of the panelists. David, I turn the virtual floor over to you.

David N. Tente: Thank you, Dave, for the kind introduction and the opportunity for ATMIA and its members to participate in this webinar. I'm sure that many of you attending today are already familiar with ATMIA, the ATM Industry Association. For those who are not, we are a global, not-for-profit association that represents the interests of the entire ATM industry. The largest single segment of our membership is ATM deployers and operators, which includes the largest commercial banks, community banks, credit unions, and also independent operators of all sizes.

In addition to hosting the world's largest ATM-focused annual conference, we also advocate for an ATM-friendly regulatory environment, develop operational best practices, offer basic ATM channel online education, and produce a wide variety of industry reports. ATMIA membership is open to any industry stakeholder. The US is by far our largest region, but we do have over 11,000 individual members representing over 500 organizations that are based in 66 different countries.

There's one additional dimension to ATMIA, which has become quite important: we also own and operate the ATM Security Association.

After the rest of the panel has introduced themselves, I'll be leading off the discussion with some information about general ATM crime trends

here in the US. I'd like each of the other panelists now to introduce themselves. And, John, over to you.

John Toneatto: Thank you, David. Good morning, everybody, and welcome to the forum. I've been with Loomis now for several decades and been running the security side of things since the mid '80s. We're heavily invested in the ATM industry. We currently run a little over 10,000 employees each day and deploy a little over 2,100 routes. We service 106,000 ATMs across the country, and annually we touch those ATMs about 5.6 million times. That comes to about 53 or 54 touches per ATM in the course of the year.

Through that, my group works on dealing with the threats and countering the threats. We break that down into two areas. Some of my colleagues will be covering this, but burglaries (against the units), robberies (attacks against the individuals), skimming, and then jackpotting are all external threats. And the internal side of it, too—my group also investigates all the internal threats. If we cross-load an ATM, if we leave a safe door open—any kind of internal theft or any kind of Ponzi scheme, as it relates to ATMs.

We are quite busy, as a group. I've got 17 very good investigators that work for me, as well as the entire claims team within Loomis.

So, going on to the next one, please.

Tente: Thank you, John. And Brad?

Brad Moody: Good afternoon. Good morning, too, wherever you are. My name is Brad Moody, with Lowers Risk Group. Some of you may have heard of our organization, but we basically work in the areas of fidelity crime, focused on risk mitigations globally. We've got offices strategically located around the world to help with the London market, specifically towards the fine art and specie markets and the remediation of risk. We work very closely with all the financial institutions and armored carriers to work with them collaboratively to work in circumventing solutions that work within their areas—whether ATM risks, or money risks, or theft risks—and we help try to condense and stop those with mitigation areas.

We oftentimes are leveraged with various industries to look at corporate best practices, to work on rewriting those practices to understand exactly the immediate threats, and then take the expertise that we have to cross-pollinate those across the industry.

Tente: Thank you, Brad. Brenda?

Brenda Born: Hi. Good afternoon, everybody. Thank you, Brad, for the pass-off. My name is Brenda Born, and I am one of the supervisors at FBI Minneapolis field office. I've been with the FBI for just over 17 years. I have a slide here just giving you a little background on the FBI. We were established in 1908. We have between 35,000 and 36,000 employees. Of those employees, about 14,000 are special agents and about 22,000 are support personnel.

Here at the FBI, we have 56 field offices across the entire United States. Like I mentioned, I am with FBI Minneapolis, and FBI Minneapolis not only covers the state of Minnesota, but we also cover North Dakota and South Dakota. And besides the offices that we have here in the United States, we also have just over 60 offices across the globe, and they cover over 200 countries, territories, and islands. And just to give you some priorities—we have a lot of priorities that we cover in the FBI, one of them being violent crime, and for me specifically, I oversee the Violent Crime Task Force, which is where the ATM violation falls under.

Thank you again for having me. I'm looking forward to the presentation, and I'll turn it back over to David.

Tente: Thank you, Brenda. And thank you all, panel. Thanks to everyone who's attending this afternoon's webinar and those who might be listening to recordings at some point as well. I'd like to lead off the discussion today with a brief, high-level overview of some of the ATM crime trends that we're seeing, and how the ATM Security Association is now able to track those trends. Everyone in our industry is concerned about the rapid rise in ATM crime. It's been growing significantly over the past year or so in particular, and it really got a bump during the pandemic.

But also, unfortunately, many of us in the industry—perhaps like yourselves—who need to know what's happening in the way of criminal activity have only had a few sources for that kind of information outside of their own fleet. More often than not, it comes from news sources. Even then, probably not unless there's been multiple incidents in your area—perhaps an explosion, somebody got hurt. The bottom line is, it's a lot harder to protect your ATM fleet if you don't know quite what it is that you have to protect it from.

That situation is changing now. We don't have enough time today to go through the history of this project, but the ATM Security Association launched the first and only global ATM crime database in May of last year: the Crisis and Crime Management Intelligence System. One of the things that we learned very quickly is that criminal activity in the ATM channel is not homogenized, by any means. The report you see here is on the home page of the Reports & Statistics section of the website. And as is displayed towards the top of the page, there have been 14,613 incidents reported from over 2,400 reports going back to May of last year, and that's the total count globally.

This data was captured towards the end of September, so it's still pretty current. You see the pie chart there shows that 75.5 percent of the incidents reported are fraud attacks, and 24.5 percent are physical attacks. Of course, when you're looking at numbers like this, you'd often want to know what type of fraud attacks are being experienced because that, again, helps you in defending yourself against these types of attacks.

Now it may surprise you to see that the largest number of attacks globally are a method called cash trapping, with card theft being in second place, followed by skimming. Skimming, which you may have expected to be in first place, is not globally.

As I mentioned a minute ago, the first thing we learned was how different these trends are from region to region. We're looking now at the US

market. The previous numbers were all global numbers (Europe actually aligns pretty well with that data). This chart is for the US market, and if you look too quickly, it's a very similar pattern to what you saw in the previous pie chart—except that the numbers here are completely flipped, in the US. We have 77 percent physical attacks, compared to 76 percent globally being fraud. So, quite a bit different in those numbers—and as I say, it does change quite a bit from region to region.

Now we're still looking at the US market here, but now we're drilling down into fraud attacks only. And it breaks down very different from what we saw with the global numbers, where cash trapping was the most common type of attack globally—it's just a very tiny sliver in the US. And although skimming is no longer the primary problem worldwide—and overall—in the industry, it's still the most common form of fraud attack here in the US. So, still very much an attack factor that we and operators need to be prepared for.

What's a little bit unsettling in these numbers is that we've got a growing problem of jackpotting, since it's up to 10 percent as you see here. Since jackpotting requires physical access, though, and we lead the world in the rate of physical attacks, it's not hard to understand why those numbers are growing.

You may have noticed, too, that a heat map has been displayed to the left of these pie charts. It shows here, for example, that California and New York are experiencing more instances of fraud attacks than other states, and we are hearing directly from our members (and anecdotally) that these two states have been experiencing a very high rate of fraud with regard to mag-stripe benefit cards.

And my last slide, we have a breakdown of the different types of physical attacks in the US. I suspect that most of you probably could have predicted that the chart would look something like this. Theft of the ATM itself has taken over as the most common type of attack. Together with theft from the ATM, they account for almost 98 percent of physical attacks. The heat map confirms that Texas seems to be the king of "hook-and-chain" activity.

So I hope with this I've given you a general sense of the high-level trends that we're seeing in the industry, and how we're able now to track that activity. If there are any representatives of law enforcement on the call today, please know that we're happy to provide you with free access to this system. It's really very helpful for the whole industry, and law enforcement itself, to be able to have a way to share that information a little more globally, so just please let me know of your interest.

Now we're going to go on to our panel, and to John. Our panelists are going to be able to fill in a lot more of the details surrounding these issues, and I'll turn it over to them.

Toneatto: Great. Thank you, David, I appreciate it. Interesting note that—and I'll talk about robbery a little bit—that some of the robbery trends we have around the country match some of the events that show up on your data as well, in terms of concentrations in Texas and concentrations in California. ATM personnel attacks—obviously, extremely dangerous. It's what we face every day, as we go out and service ATMs.

One of the biggest distinctions between the United States and the European Union is that we have a high number of drive-up ATMs here in the United States. Most of the ATMs serviced overseas are done in either kiosks or in-wall ATMs, while most of our ATMs are done in a drive-up or a standalone kiosk. That puts us at a little more risk as we're servicing these units. So go on, please.

The targets that usually are threatened in one of these attacks are the CIT [cash-in-transit] carriers that replenish the ATM. There's a certain amount of time we spend doing these tasks, and we're exposed. And also the FLM providers, the group that goes in and clears cash jams and goes in and fixes the ATMs if there are any issues with them—as they approach an ATM or go inside an ATM, they're also exposed to that.

Several of the banks that we deal with have their own personnel conducting deposit pulls. Whether they go into the ATM daily or every other day, if one of the CIT carriers doesn't do that, the banks are doing that. And of course, when they access an ATM to do a deposit pull, they're also exposed. The location, as I said earlier, for ATMs—we occasionally get attacked at in-wall ATMs, but most of our attacks (about 95 percent of them, as it relates to ATMs) occur at drive-up ATMs or in standalone kiosks.

And to give you an idea how pervasive it is in the United States for us, in the last five years for all CIT carriers (including Loomis) there were 202 attacks—armored car robberies, attempted take down, attempted car hijacks—and 107 of those occurred at ATMs while only 29 actually occurred at banks. So the perpetrators of these have identified that it's a better solution, an easier attack position, to do that—and I'm going to show you a slide in a little bit that will kind of demonstrate that.

Very high level of violence in these attacks: 37 attempted homicides over the same period of five years, with four carrier employees killed and two bystanders killed in attacks. So they can be extremely violent, extremely dangerous, and that's what we're dealing with on our countermeasures in approaching this. So, next slide please.

I took one of our attacks that occurred last year to kind of demonstrate how quickly these occur. Our tech leaves an armored truck—you can see how we park the truck very close to the ATM, so we minimize the distance between the truck and the ATM. And while she was in there, about to open up the ATM to settle it, the perpetrators came up on the inside lane—the one that is used for handling deposits, and the drive-up window—pull up very quickly, they exit. This is a two-person crew that did this, against our tech. They jump out, they assault our tech on scene.

She had a bag, as you can see, to her left side. And in that bag she—by the way, she didn't have any cash in there. She was getting ready to settle the ATM. And they grabbed the bag and ordered her back to the truck. And as she's walking back to the truck, they fire a round over her head and into the truck, and then they escaped.

This entire attack took about eight seconds, very quick. We're dealing with a bunch of these right now in the Southern California area, and very violent. Go ahead.

So we've got some fairly common countermeasures that all of us use. One of them is, we've upgraded our vehicles over the last several decades. They're very high-security-level vehicles. We've been very focused in our robbery training—using different venues, using different techniques, on how to avoid these kinds of situations. We have a very specific location approach on how we approach an ATM that we're about to service, and where we park our vehicles, how we park our vehicles. You probably noticed in that previous slide how that vehicle was parked with the door that she was exiting out of right next to that ATM. That is a purposeful move on our part.

The key for us is to reduce the amount of time we're at an ATM. Unfortunately, because of servicing these ATMs, you have no choice but to spend some time. By the time you settle an ATM, open it up, pull out the cash and replenish it, there is an amount of time involved. So we try to exchange currency in as secure an environment as possible. Sometimes that will occur in the back of the truck, sometimes that will occur in the kiosk (if it's available). Unfortunately, sometimes that's right there at the ATM itself, where you're exposed.

So as we deal with our customers and the ATM owners, we talk about that. We partner with them to kind of cover this and reduce the threat. We want to reduce the steps needed to service an ATM. When we first started in the ATM market, there were probably about eight or nine settlement schemes used to go in and settle an ATM. There are well over 80 now. So, our crews have to spend a lot of time as they move from ATM to ATM, and refamiliarize themselves that you have a different approach as you settle that particular ATM.

Ensuring good coverage—CCT coverage—around the ATM is critical. As you can see, that location we were dealing with had very good coverage. In addition to what we had on our vehicle, that helps us in the investigation side of this after we have one of these events.

And monitored alarms in place. These are in place in a lot of locations where they're monitoring, they have alarms monitoring the ATM, so when you open up an ATM, it's monitored. And they have a hold-up feature within that, that will allow one of my people to send a threat alert immediately. So, go on, please.

I wanted to bring this up—this is more of an attack against the unit, which one of our other colleagues will be covering later—but this has become a big trend in Europe. They've had gas attacks on ATMs. They're pumping fuel and oxygen into these, with a detonator, and they're literally blowing out the ATM from the front to access the cassettes that are inside, as opposed to the in US, where we have drive-ups and they attack us. In these cases, there are a lot of attacks against ATMs. Go on, please.

Again, this will be covered by one of the other colleagues on the panel, but one of the things that we've seen is we respond to these from our customers when they call us and say, "Hey, we have an ATM that's been attacked." One of our customers had come up with this—there are several companies that produce this kind of security ATM, so it can't be attacked from a hook-and-chain point of view.

And an armored car crew will arrive on scene. They will have the key to open up that gate so they can open up the ATM. Some of these are very, very sophisticated. They come in remote monitoring that when you open up that gate to access the ATM, they're aware that that's being opened, they know how long it's open, and they can react to that from a remote perspective as well. Go ahead.

I talked about how we really approach things from two points of view. One of them is the external attacks, the robberies, but we also have internal attacks that we attempt to cover. Unauthorized access to safes—very simple countermeasures we put in place, we use auditable locks (one-time, encrypted locks), good coverage of CCTV at the ATM, and with monitored alarm systems—all help detect any kind of unauthorized access to a safe other than when we're in there servicing it.

This is a straight internal issue for Loomis and other carriers that do this kind of work. There's been an explosion of multi-denomination ATMs in the system, and as a result of that we occasionally put the wrong denomination in the wrong cassette. So our countermeasures we put in place in working with our customers are: make sure that they're properly labeled, the cassettes are properly labeled, both inside and out. That the cassette slots, if the machine is driven off of where the cassette is put into the machine, are properly labeled. And we always work with our customers to try to limit the number of denominations that they're using in an ATM, because not only does that create a potential of this type of loss, but also the longer we're moving different types of denominations to an ATM, it's that much more time we're spending out there.

Internal theft is something we all face and we deal with. Again, we use auditable locks with these encrypting schemes. We've got very good arrangements with the FLM [first-line-maintenance] providers who may also access the ATM during the cycle of a loss. We've got excellent investigation protocols on this, and we constantly train our investigators on how to deal with that. And what we do to countermand any potential internal theft is we do a whole bunch of random ATM audits every day. We go out and randomly audit ATMs after they've been serviced to make sure they're in balance, that all the money was put in properly. And then on a regular basis, we randomly swap our ATM crews.

And with that, I'm going to turn it over to Mr. Moody for his side of the presentation. Thank you.

Moody: Thank you, JT. During this side, we're going to talk about the new kind of bank robbery and cyber fraud, and some of the definitions and some of the occurrences that we're seeing. And to reiterate what David had said earlier about the new ASA data: it's very, very good data to have, and it really does help the industry. So we continue to encourage people to use the tool. David, we can go to the next slide, please.

So again, the next form of bank robbery. Some of the things that we're going to talk about within my segment—cash trapping, we'll describe all those, and skimming—I think we all know what skimmings are. Jackpotting is a very popular term now. I'll describe why that one is of

significance. The same with how deposit trapping and cash trapping go hand in hand. Fraudulent deposits—I think we may have seen the old times where people would put wet money, wet $1 bills, in there and they would say, "Hey, I deposited $400" instead of 10 wet $1 bills, to create that fraudulent deposit.

And then the mobile app compromises. This is very new, in the advent of the walk-up ATMs with the mobile app authentications. Next slide.

So it makes you wonder—why is there a huge advantage with cyber compared to just, unfortunately, robbing the CIT carrier or the independent ATM owner that's filling, or even the bank that's deploying deposits or replenishing their own ATMs? Well, you don't need a weapon, so you don't really need to have that show of force. The tools that you need, you can actually buy all the tools from the dark web. It tells you exactly what to do—by the product name, by the ATM model—exactly the tools you'll need, and where and how to do the crime.

You don't have to interact with people, so you'll see someone will go in at two o'clock in the morning and they'll empty the machines, or they'll go in and they'll use the drilling techniques to implant the jackpot devices. This is considered a property crime, so if you were convicted of skimming an ATM or jackpotting an ATM and you get hundreds of thousands of dollars, it's a property crime whereas if you go through and you rob your CIT carrier, that's a much harsher crime and very much stiffer penalties.

The speed that it is done within this is incredibly fast, and it's hard to trace—so a lot of things that happen, you really can't nail it down very easily. We can go to the next slide, please.

So this is what we see through the data that's out there. And I can explain why it has such a sharp increase, but one thing I want to make sure we identify is, I don't want this to falsely say that in 2022 something great has happened, or "Hey, look, we have a decrease." That number is only through the end of April, so if we were to add the current time, it would be almost a straight up-and-down arrow at this point. And so the natural question is, "Well, that's interesting. And so why is that?"

The simple answer is, a lot of the operating systems that we're running to support the ATMs—those are no longer supported. So now you look at the security patches and updates that are within the machines are no longer available, so that creates an exploitable event. And so the cybercriminals are able to again identify, by the types of ATMs, exactly how to exploit that. So unfortunately, we see this kind of existing to increase. However, the manufacturers are doing some great things in making the access devices a lot harder to access, or where the simple tools won't work.

And then also, banks are putting in a lot of details that are out there to decrease the abilities. There are also some countermeasure activities that are going on. There's actually even one device that we feel very strongly and very passionate about, that you can actually implant the device inside of a cassette. It's very small. It's about the size, a little bit larger than the size, of a cell phone—but it can actually listen for certain identification marks, so it can listen for drilling events. If it hears a drill, it sends an alert to the bank's SOC [security operations center], and then it also will disable the machine, turn the machine off.

So, little things that are there. If it hears a tug, or somebody wrapping a chain around the ATM, it can turn it off and alert the security operations center. So, these are exciting things that are now coming out to happen. Next slide.

Breaking down what's going on in the world itself: as David said, about 30 percent—27 to 29 percent—of the events in the US are cyber, and the rest are physical. So, Americans would much rather rip the ATM out of the ground, because, as JT said, there are no real drive-through areas in other parts of the world. The drive-through ATM and the kiosk ATM are very selective into the US market. It's not a lot of "through the walls."

You can't really wrap a chain around something that's inside a wall. It's fun to watch them try, but it doesn't really work that way. But then when you look in the areas like South Africa, where it's just so simple to just have 18 people with automatic rifles enter into a shopping center, and they just start off very violently. They start off shooting because it's easier to get the money. The quality of life and the assurances of life there just don't exist as they do otherwise.

But we do see an increase in the cyber world coming in. The interesting thing about the cash trapping—I'll kind of describe that, why that's such an important piece, and why it's a little inverse relationship within the US. Cash trapping is as simple and as elegant as gluing the trap door shut on the cash dispenser. So someone goes in, they put an adhesive on the cash drawer. They watch three or four people go through, remove cash, and the door doesn't open. So you see them, you see the customers, they can't get the cash out. They get frustrated and they go inside the banking center, or they get frustrated and they walk out.

So right behind that is someone comes in with a pry bar, and they pop that door open and they remove the $200, $300 that's trapped behind the door. So very low limits of cash, but that's the easiest and most elegant way that cash trapping is happening.

Skimming is not going away. The devices are getting thinner and thinner, so where we used to see where the card readers—you would see it's modeled, it looks exactly like the manufacturer's card reader. Now, the internal components that are inside, the thickness of them are half the size of a dime. So when you look at that, they're able to internalize the skimming device itself and the PIN reader that goes inside the fascia, with a camera—you can barely even see that it exists. So it's very, very unique, and they're getting much, much better about the fascia, replicating the fascias.

Card theft is as simple as, they're putting in the same kind of devices to trap the cards that are inside. And they go through there and they pop the fascia off, and they pull the cards out of it. And they also have your PIN number at the same time, because they've seen you try to enter it into the

ATM. We can go to the next slide, please.

So again, looking at this—jackpotting is not new, obviously. The first time it happened in the US was 2018-ish. The first known event was in 2015 in Mexico City, as far as we know. But why this is an important thing—when you look at it, it's only 0.3 percent of the problem—but when you look at the amount of cash that's taken, it's actually the most lucrative way that cash is being taken. Dispenser jackpotting is as simple as, they drill a very small hole into a strategic location, they insert an endoscopy scope to find out where the actual USB tray is, and then they go through and they enter in a device and they load malware onto the machine that's going to turn that machine into a jackpot—or it's going to start dispensing cash and it won't ever record those actions.

The other way that it's happening is they're actually replacing the motherboards with a with a piece of equipment that will take certain key indicators, but it actually reverses transactions. So as they go through and the actors are removing cash from the machine, they're entering a sequence of numbers and it actually dispenses the cash, but it never records on the EJs or any kind of electronic journals or anything that's out there. So that's why that's an important piece of that, to make sure that it's all understood. We can go to the next slide.

So here are just some pictures, graphics, examples. The one on the left is glued cash, which is interesting on the US side. It's much easier for the European markets and Canada, where it's polymer cash (it's easier to remove the glue itself). That card skimming device is one of the older ones—I need to update my deck—but the new ones that we've just found, the new ones are very, very thin. You can't actually even see that it's there.

I would stress for the FIs to understand that, to have a clear card skimming procedure with their employees as they're cleaning and inspecting ATMs daily—as they pull, if they notice something, to have a very clear procedure in there because typically when someone has a card skimming device, they are sitting close in proximity with a Bluetooth where they are actually recreating cards in close proximity to that.

So some people could argue that the banking center employees could be in danger if they pull off the skimming device and they hold it up like, "Hey, look at this"—well, that costs money and the gangs, the mules, they want to have that back because they're personally responsible for them to pay back their person that's hiring them to perform these tasks.

And then cyber jackpotting—so this is, again, where we are implanting code into the machine to dispense currency at a very, very fast rate, within a matter of minutes. You can actually dispense $500,000 out of an ATM in a matter of less than two minutes. So that's why this is a big, significant thing. We can go to the next slide.

And I'll turn it over to Brenda. If you can, please talk to us about physical attacks.

Born: Great. Thanks, Brad. Like David had mentioned earlier, that during COVID, we saw an increase in ATMs being targeted with banks being closed during the pandemic. One of the other things we had seen an increase in during 2020 was also banks and ATMs becoming targets during civil unrest. As there was civil unrest across the United States, we saw the increase in banks and ATMs being targeted.

In looking at 2022, the top three ATM physical attacks that we are seeing in law enforcement: number one remains the hook-and-chain tactic that is used where they are getting a chain, in the area they're at they are stealing some type of truck—a lot of them have been Ford F-150s—and they are using the truck with the chain in order to gain access into the ATMs.

The second tactic that we are seeing is brute force—brute force with using crowbars or pry bars, saws, blowtorches, some type of power tool or hand tool, in order to gain access into the ATM. And then the third—John had mentioned it—was related to the vendor and technician robberies of those trying to service the machines. One of the other things we are seeing during 2022 is that while the hook and chain remain the top tactic used, we have seen a little bit of a decrease in that tactic. But we've seen the increases in the brute force and the attacks on vendors and technicians with it.

I know David had mentioned early on, the connection to Texas when looking at physical attacks. One of the other things that we are seeing related to Texas is, while they continue to be the top state with the number of physical attacks on ATMs, we are also seeing a connection with those individuals that are traveling outside of Texas and committing these crimes in other states. I know here in FBI Minneapolis, we have had connections related to vendor/technician robberies, as well as to hook and chain, with individuals associated in Texas.

One of the other things that we have seen impact the physical attacks related to ATMs is the power of social media—social media showing, like John had mentioned, the security mitigation measures that can be implemented to help protect and try and deter those individuals from gaining access to the ATMs. As the subjects of our investigations, as they analyze and look at those mitigation measures, as soon as they find a way to bypass those, they are posting those out on social media. So what we see then is within the next 24 to 72 hours, we will see an increase related to whatever was posted out on social media, whether they're posting a way to do it with the hook-and-chains, or whether they're posting ways to look at bypassing the mitigation measures that have been installed at the ATM.

In looking at it from a federal perspective, which is what I would be doing as part of the FBI, our local partners would be the first on scene with it and they would reach out and collaborate with us, from a federal perspective. We would then look at opening an investigation and assisting with the investigation and trying to determine those that were involved in the ATM incident. But when it comes to federal prosecution, it would really depend on the jurisdiction of the US Attorney's office, on where those specific criminal acts took place.

For example, here in FBI Minneapolis, in the state of Minnesota, looking and working with the US Attorney's Office here in the District of

Minnesota, while we would open a case and we would assist our local partners, in terms of prosecution, the things we would look at would be serial offenders—looking at their criminal history, any ties to gangs, as well as any level of violence—was a weapon used? Was anybody injured during the incident?

So all those would come into play in determining where would be the best place to prosecute an investigation as it moves along, and individuals have been identified. Is it better at the state level, or is it better at the federal level, in terms of prosecution with it? So, those are the types of things that we would look at in terms of prosecuting those cases.

I will turn it over to Dave, and we can see what kind of questions we have from the audience.

Tente: Thank you, Brenda, and I'll turn it back over to Dave and his staff to handle those questions. Thank you.

Lott: Thanks so much to all of you; very informative presentations there. Jessica has some questions that have been submitted that we're going to pose to the panelists.

Jessica Washington: Thank you. I believe this question goes to David: Overall in the ATM industry, what do you think the primary cause is for a steep increase in ATM crime?

Tente: Well, we honestly think that one of the biggest reasons that we have there is just the fact that the penalties are so low. It's a very low-risk type of crime. We're seeing that most of these, it's on the state level, so that even if you're caught and convicted, it's a property crime—and Brad had talked about that as well. It's maybe not that much different than stealing a six pack of beer from the convenience store, from the standpoint of penalties. So we think that is probably one of the root causes. It's just an easy crime, and very little consequences.

We see now that at the federal level, they've introduced a bill to make that a felony with up to 20 years in prison. So we're hoping that that bill gets passed, and maybe we'll see some changes in the trends here.

Washington: Excellent. Thank you.

Born: Jessica, it's Brenda. Can I jump in there for a second?

Washington: Yes, please do. Thank you.

Born: Just to reiterate what David has said, in addition to that and working to determine where is the best to prosecute, whether it's at the federal level or state level—like David had mentioned, if there's no level of violence with it, there's no weapon used or somebody getting injured, then it does move more toward the state level. But one of the other things impacting that is, depending on the communities that are hit—looking here at FBI Minneapolis, where we have a significant increase in violent crime, that does come into play in terms of what resources, whether it's at the county level or it's at the federal level, that they can and do have available to them to work these types of investigations, from a prosecution perspective on it. I just wanted to point that out.

Washington: That's great. Thank you so much. And please, if anyone can answer, as we go through these. The next question is: Is there an option to install a gas or explosive monitoring device to alert for a gas attack?

Moody: I can take that one. That's one of the indicators I had said that there's a fairly new device that we're currently in testing with, that it hears and it learns behavior—so any kind of drill or any kind of thing that's out of the ordinary, it can actually hear that and then shut the machine off and notify. So those oxyacetylene explosions—it's still going to happen, but at least it's going to notify before it happens, so you're able to get more footage.

Washington: Excellent. Thank you. And maybe this is for John, but anyone, again, can answer: Is there a time of day when these armed attacks are most likely to occur?

Toneatto: Yes. Actually, they can occur at any time, but generally most of the attacks that we see are between 9 a.m. in the morning and 1 p.m. in the afternoon. They happen earlier in the day, and actually earlier in the week as well, in case you're wondering about that as well. Monday is usually the busiest day for attacks, followed by Tuesday and Wednesday. And again, it can happen any day of the week, but generally that's when we're seeing the attacks occurring.

Lott: Can I jump in with kind of a follow-up question for all the panelists here? In terms of these attacks that are occurring, are these local gangs or is this a very coordinated, organized, more regional—or national—effort going on?

Toneatto: I know in the recent string of attacks we just dealt with in Los Angeles—three attacks in a row, in less than 45 days, all by the same gang (they just took them in custody, by the way. Did an excellent job)—the VCTF [violent crime task force] here took care of that for us, by the way. Excellent work on their part, along with the sheriff's department.

But yes, they tend to be localized. What we've seen in the Texas market—Texas and New Orleans, and some of those neighboring states—for a period of time, some of those people that were perpetrating those robberies would originate in Texas and then move out to some of the local areas outside of Texas. And because of the concentrated effort by law enforcement in Texas, they would go over to Louisiana, go up to Oklahoma, and attack in those areas as well.

Generally, they are gang-driven. And unfortunately, it's not exclusive. I know that in Los Angeles, we're looking at several gangs that are doing

attacks. One of them has already been taken into custody, and we're working on the rest.

Washington: Excellent. Thank you. This is a two-part question: What are some effective physical measures to defend against the smash-and-grab or the hook-and-chain ATM attacks? Bollard poles don't seem to prevent these attacks—and in the hook and grab, are they able to open the money chest?

Lott: Who wants to take that one?

Moody: I can opine on that a little bit. We noticed that when the big banks started using the crossbars, especially in the Houston area, they dropped significantly—so that those weren't occurring (until they just figured out how to break the bars off, and then steal them). It's really about around those construction areas, where they're using construction equipment, and fairly organized, where they can pull the ATM off its foundation.

What I can say from the other chain gangs, it's really just about the placement of the ATM, and to put effective countermeasures around it—meaning, if you have an ATM that's in the convenience store, that's not bolted down properly, that's towards the glass itself, then it's in a high-risk area for it to be stripped out. The bad guys are typically fairly lazy, so they're going to go to the path of least resistance. And smaller ATMs, they weigh less.

The other side of it is that until the banks start effectively using appropriate cash management to where they're not filling ATMs full of cash, they're not appropriately forecasting the cash. A lot of the ATMs don't need that much money inside them to begin with, so there's less at risk that way as well.

Toneatto: I would add that some of our customers that we deal with have also deployed GPS trackers in their cassettes that have been effective in...it's more of an "after-the-fact" issue than to stop it, but it helps you mitigate it after it occurs, and that's been effective. As I said when I spoke, I think it's very important to have good CCTV coverage in and around that area so that you can see what you can glean from that perspective.

Washington: Great. Thank you. I have a feeling this question might cause some dialogue: When will more in the industry stop authorizing withdrawals on fallback transactions? If the issuer won't authorize, then the fact that the card is compromised/skimmed is moot.

Tente: I guess I can comment on that a little bit. I'm not necessarily an expert, but I do hear from our members—primarily independent operators—that the fallback requirements keep shrinking and changing, as far as the limits that they're allowed to go to here. That's causing some problems, just because some of the operators now have to think, "Do I want to risk exceeding my fallback limit, or should I just turn down this transaction and not take it at all?" I don't have a solution for the problem, but I recognize that it's out there, and we do talk to the card schemes about it on a regular basis and try to make sure that those things are equitable and makes sense across the board. But I know where the question is coming from, anyway.

Washington: Yes, and there's kind of a follow-up/similar question: Does tapping your card versus inserting your card at the ATM prevent skimming?

Moody: Yes. Tap is a different type of cybercrime completely. Skimming is when they're actually catching the details of the card itself and defaulting to where they use the PIN number to validate.

Lott: But I guess the follow-up question, Brad, would be: Have there been any incidents where people have put, like they do on the card readers (false card readers), they put some sort of fascia over the tap reader and they're trying to intercept that near-field-communication data?

Moody: Yes; David, you may know more about the near field, because that's fairly recent in our data collection.

Tente: Actually, I'm not sure whether or not that data comes through on that. We've had eavesdropping types of attacks—that's a little different type of attack, of course, because that's mainly on the read heads—but whether or not the same concept could be used on the contactless, I don't know the answer to that.

Lott: We'll do a little bit more research on that, because I know in near-field communication that data is encrypted—plus, it's using generally a token instead of the real account number.

Tente: Right. Yes.

Lott: Well, we're approaching the top of the hour here; I want to thank each of you—David, Brenda, John, Brad—very insightful commentary on this issue that I know is of great interest. I want to thank our audience for participating, with your attention and your questions. Just as a reminder, a recording of the webinar (as well as the presentation deck, and a transcript) will be posted on our website here within a week.

We would ask the participants to respond to a survey that's going to pop up at the end of the webinar. We use that survey, as I had mentioned earlier, to provide valuable feedback to make sure that the content that we're providing is of value to the audience, as well as to ask you what topics in the future you would like us to address.

I'll take just a minute to put a plug in: next Thursday at the same time (one o'clock), we have another webinar—our third of the year—on the financial exploitation of aging adults. And then we'll do our year-end "Payments in Review" wrap-up, a traditional webinar that we do at the end of the year, and that will be on December 15. I hope that everyone will register for that, as well as subscribe to our weekly blogs to keep posted on these types of payment issues.

Thank you all for joining us today. Take care.

Send questions about the webinar to David Lott at david.lott@atl.frb.org.

You may view previous *Talk About Payments* webinars.