## The Year in Payments

**Transcript**

**Jean Roark:** Hello, and welcome to the Federal Reserve Bank of Atlanta's *Talk About Payments* webinar. Today we'll discuss, 2019: Payments in Review. I am Jean Roark from the Federal Reserve, and I'll be your moderator. Before turning our call over to our speakers, I'd like to turn to slide two so we can run through today's call logistics.

If you haven't joined us through the webinar yet, click the link you received after registering. For the best webinar experience use the FAQ document, which can be found using the **Materials** button in the webinar player page—but I'll highlight just a couple of important notes for you.

You can listen to the audio through your PC speakers or through your phone. If you use the phone option, slides will not sync with audio unless you change one setting. To do that, you can select the gray gear located on the upper right corner of the slide window just above the presentation. From there, you should see a few options in the media chooser, and you can select the phone option. You'll only want to change that setting if you are listening through your phone.

You can expand the size of your slides, and to do that you can use the **Maximize** button in the upper right corner of the slide window—and that's located on the webinar player page. If you'd like a PDF of today's presentation, you can access it using the **Materials** button.

We'll be taking your questions throughout today's presentation, and you can submit them at any time during our call. If you've joined us via the webinar, just use the **Ask Question** button on the player page, or you can always email us at rapid@stls.frb.org. Either way, we'll get your questions queued up for our presenters today.

And with all of that out of the way, I'm going to turn to slide three and turn it over to Dave Lott.

**Dave Lott:** Thank you so much, Jean. As Jean indicated, I'm Dave Lott of the Retail Payments Risk Forum here at the Atlanta Fed, and I'm joined by two of my colleagues, Jessica Washington and Doug King. However, the discussion that we're going to facilitate today comes from a collaboration of the entire Risk Forum team. Unfortunately, we couldn't all fit around our table today, so you have the three of us.

For those of you that may not be familiar with the Retail Payments Risk Forum, let me take just a minute to review that really quickly. The group was created back in 2008 as part of the Atlanta Fed's risk and compliance division. We really have a threefold mission: that of research, education, and convening groups. In addition to our quarterly webinars, we have our weekly *Take On Payments* blog that I hope that you all are subscribers to—and if not, please join us there.

We also produce various white papers and research studies, some of which we're going to touch on later in the discussion today. All of our work is available at no charge and on our webpage at the Atlanta Fed website.

So before we get into the material, we have a little polling question that we wanted to ask everyone to get started to better understand our audience. Jean?

**Roark:** Thank you so much, Dave. Let's pose that first polling question for our group. You should have a box that pops up on your window, and I'm going to look on my participant view that I have here in the studio in St. Louis. I see that box so I'm going to read that question aloud for you, and we'd love it if you would give us your response. So the question is: Do you think the criminals are winning the war on payment fraud? And your possible responses are: yes, no, or both wins and losses.

So you have a couple of options there, and I am just going to stall for just a couple of seconds to see if we can get as many responses as we can. And I see a whole bunch coming in, so Dave, just give me a couple of more seconds. All right, so we're going to stop that poll and show the results. So those results popped up on your screen already. So it looks like, Dave, 57 percent of our participants said C, both wins and losses, and 33 percent said yes, and just 10 percent said no.

So I'm going to turn it back over to you.

**Lott:** Well, that's a very optimistic group, I think. Doug, do you want to kick us off and talk some more about some of the specific schemes that we're seeing?

**Doug King:** Absolutely. And hopefully by the time we get through with this, the optimism will remain with this group—or perhaps even be more optimistic, but that could be a challenge given those numbers. But in my opinion, the two biggest fraud or payment crime stories in 2019 were ransomware and business email compromise. I don't have time to go into detail on the ins and outs of how criminals are pulling off these attacks, but I do want to share some statistics and just high-level thoughts about ransomware and business email compromise.

So ransomware is a form of malware that encrypts files on a victim's computer or server, rendering them unusable. Cybercriminals demand a ransom in exchange for providing the encryption key to actually decrypt those files. Based on figures from several different security vendors, in 2019, ransomware has impacted approximately 85 school districts—and that includes over 1,200 schools—and then you can throw in additional universities and colleges as well to that mix, 100 municipalities, and 700 healthcare providers.

On top of that, there have been thousands and thousands of SMBs [small to medium-sized businesses] that are not included in those figures. And then in the last few quarters, we've seen a big uptick in a newer target of managed service providers, where the criminals are going after these managed service providers who perhaps provide cloud services or data services to hundreds—or in some of these cases, thousands—of smaller enterprises.

So in the third quarter of 2019, just to give you an idea about what are the economics behind this, the average ransom payment was a little more than $41,000, which was six times higher than it was as of December of 2018. And there are different variants or strains of ransomware, but with one strain—the Ryuk—ransom payments during Q3 of this year ranged from $268,000 to $377,000. During 2019, we saw some ransom demands that were north of $1 million. Generally, these ransom demands are based on the value that the criminals perceive the data that they're holding ransom to be.

Whether you pay ransoms or not, the victims suffer economic costs as well as hardships. But according to one county's chief information officer, whose school system was hit with a ransomware attack, he estimates that the average ransomware incident costs approximately $8 million and takes 287 days for the victim to recover.

And unfortunately, taking my optimistic hat off, it's getting worse for the victims with news out just this week that some of these criminal organizations behind the ransomware attacks are establishing public websites that are listing entities that have been infected and who refuse to pay their ransom. And they're even going so far as to putting some of the data in the files that they've encrypted into the public domain. So really ransomware is also becoming a data breach and a dump problem. I think we'll spend a little bit of time on data breaches here in a second.

Jumping over to business email compromise—or it's also referred to as email account compromise—which is a sophisticated scam that targets businesses and individuals who perform transfer of funds requests. The scam is carried out by compromising a legitimate email account or personal email account through social engineering—or we've seen a lot of computer intrusions—to then conduct an authorized transfer of funds. The FBI came out with numbers in third quarter of this year, from a three-year period (June 2016 through July 2019). Business email compromise, or email account compromise, was responsible for over $26 billion in global losses.

FinCEN put out a bulletin earlier this year saying that here in the U.S., business email compromise has been responsible for $9 billion in attempted theft. The top sectors that are targeted in these BEC scams are manufacturing and construction, commercial services—which would be your accounting, your attorneys—and then finally the real estate sector. We've really seen an uptick lately in the real estate sector as being a target for this BEC, or email account compromise.

And then in terms of the wiring and the transferring of funds, it is generally a wire though we have seen ACH used. We've seen even gift cards being used when the dollar values are a little lower, but most of the funds from a wire transfer or ACH are flowing domestic through money mule accounts, and then from the money mule account being sent internationally.

Before I turn it over to you, Jessica, I want to just briefly touch on a new variation of an advanced payment scam that has recently been in the news. While ransomware and BEC are tied to electronic crimes, as were traditional advanced payment schemes such as—we've all seen the email claiming that we've won the lottery or the Nigerian prince has left us an inheritance. But these most recent advanced payment scams are targeting individuals through the phone with an initial robocall, and then contact continues with the victim through the phone with someone posing as an FBI agent or a DEA agent.

And the gist of the scam is that the victim's social security number has been compromised, it's linked with numerous bad accounts or bad loans, and then there are criminal activities associated with that individual and the person is facing arrest and asset forfeitures. They're led to believe that their assets are in danger of being wiped out unless they're safeguarded. I think it was two weeks ago The Wall Street Journal had an article highlighting one victim's story, and she lost nearly $340,000 in a matter of days to this scam.

So with that, Jessica, I will hand it over to you to continue with slide five.

**Jessica Washington:** Thanks, Doug. I'm going to start off with a headline. My headline is payroll fraud, and I want to highlight two areas of payroll fraud today that are really other channels that we're seeing developing. First, to tie in to business email compromise—we definitely could spend all day talking about that topic, but I want to mention another way that bad actors are sending these emails. They're posing as an employee who has the authority to change paychecks, or it's the employee themselves that they're posing as. And they'll reroute those paychecks to another account, or maybe they even just add a new fake employee altogether to send those funds, those payroll funds, to the compromised mule account.

So they're chipping away at a few thousand dollars at a time, and it's successful. Anyone who works in payroll—or anybody who receives a payroll—understands how critical these types of payments are. It's incredibly important that they're delivered timely, when promised. People get very angry when payroll is not delivered. So this is a very successful new channel of fraud, and more time should be spent on talking about risk controls on this topic.

So the next story I want to point out and pull out some things of concern is, again, a payroll story. This one is: MyPayrollHR in September closed its doors, and they were a payroll management company. Thousands of the companies that they represented and a quarter of a million workers were left with failed payroll delivery when they closed their doors. When I read that headline in September, I thought immediately it was a cyberattack, but surprisingly, it was an insider threat from the CEO himself.

So in this case—usually the payroll funds would move from MyPayrollHR through their payroll processor—the CEO redirected $26 million in payroll funds into his personal account. The payroll processor was essentially duped into sending the payroll funds, or they thought, you know, it was business as usual. So the funds moved on to most of the employees' accounts. However, when the payroll processor realized that the funds were not there to back the ACH file, they then reversed the funds. So obviously prefunding was not necessarily being conducted, and prefunding is one of the top risk controls in payroll, or sending credits. Or perhaps they were sending balanced files, where you send the credits out in the same file and maybe perhaps a funding debit at the same time, where they didn't realize the loss.

But regardless, standard ACH risk mitigation techniques were not in place, and should have been. The processor did end up reversing the funds, but most of the employees were made whole. I've read that 90 to 98 percent of the employees were made whole, but some of that at a loss to the businesses that were customers of MyPayrollHR. So an old-fashioned kiting scheme, actually.

And so that brings us into—let's talk about data breaches while we're on the topic of fraud. This year, in 2019, data breaches, already over four billion records have been breached so far—this is from Norton—and that's a 54 percent increase from the first six months of 2018. Out of the four billion records, that represents 3,800—the number of publicly disclosed breaches.

And of course, I feel like we say this every year, but we have the biggest one in history to talk about today, and that was Capital One—and also an insider threat. A hacker named Paige Thompson infiltrated the servers of their cloud storage—this was back in March—and was able to dump 106 million records. This was information on credit card applications from both consumers and businesses, and it contained names, addresses, ZIP codes, phone numbers, email addresses, birth dates, and self-reported income—in some cases, credit scores, credit limits, balances, payment history and contact information. Also 140,000 social security numbers, and 80,000 bank account numbers (however, no actual credit card numbers or login information).

So it's believed that there hasn't been much fraud occurring from this breach. However, it is the largest. But they are expected to suffer $100 to 150 million in costs related to that hack.

And I do want to mention, if you look at the slide here. This was a historic event and it was insider theft, and this is based off of the Identity Theft Resource Center's annual report. We are awaiting 2019, so this is from 2018, but you'll see insider threat is only 3 percent. So you need to remain vigilant of that threat in data breaches as well as the outside threats.

The next topic we're going to go to is synthetic identity payments fraud. And so I'll point out here on this slide right away that the amount of availability of public information (PII, or personally identifiable information) is based on the data breach. And so it's all available, and so fraudsters can easily string together synthetic identities, which usually contain some legitimate information like a social security number they will build on, and they will attach made-up information to a social in some cases. We have seen this increase because it's able to pass KYC [know your customer] and customer identification programs because they understand the requirements of those programs.

So the trouble with synthetic identities, as it relates to payments, is the payment will look legitimate—so fraud controls, typical fraud controls, will be surpassed. And so I think with synthetic identity fraud, as we see giant increases in this type of fraud—we say this a lot, but it's really going to take a collaborative action of all industry stakeholders to work out how we are going to fight this fraud. The Federal Reserve Bank, as you can see on this slide, has published several reports and has remained very active in this area, so please look to our website for more information.

**Lott:** The final area that we wanted to specifically talk about is in the area of the ATM fraud and attacks. We're all familiar with the early days, where the brute force attacks that still go on today, where Billy Bob backs the pickup truck up to the ATM, attaches the chain and tries to pull it out of the wall, or crashes into the store and they try and use that brute force to remove the machine, and then at an offsite location break into the machine and get access to the cash.

But more importantly, and at a higher loss rate, there has been occurring—not just in the United States but really in foreign countries, particularly Europe and South America—the use of explosives, either things such as dynamite, C4, or explosive gases, in order to basically blow up the surround of the ATM and expose the cash vault so that the money can be removed from that.

And then we're having the technology crimes associated with jackpotting and cash-outs. Jackpotting is where an individual posing as an ATM service technician gets access to some of the operating system components of the ATM and injects malware, which then they can come back later to the ATM and by pushing some certain sequence of keys on the outside of the machine, in essence have the machine just start spitting the currency out until the machine is empty.

Kind of related to that are the cash-outs, where it's not an attack on the ATM itself. It's really an attack on the card management system of the financial institution, where the criminal has hacked in and gained access to the card management system so they have the ability to alter balance files and any kind of transaction counters that normally are used to limit the number of transactions that can take place.

And they have an extensive money mule network and a very carefully synchronized attack to go to ATMs throughout the world and, using cloned cards or in some cases even chip cards that have been opened under false accounts, to be able to go in and start withdrawing money constantly with the criminals resetting the transaction counters and the balance files so that the transactions continue to get authorized. There was a recent case in India resulting in almost $2 million being taken out from that.

We also have the skimmers and the shimmers being put into the ATMs. There was an article today and some more recent FBI/Secret Service warnings about these devices being placed on the card readers in order to gather that information. So all of this does provide somewhat of a pessimistic look at things. So is there anything that we can look at on the bright side?

Looking at slide eight, we think that there are some things. Certainly there are some new fraud tools that are emerging, particularly in the card-not-present world, with regard to 3-D Secure and Secure Remote Commerce. We have tokenization that has taken place with the various pay wallets, and we're seeing tokenization extend to card-on-file transactions as well.

Of course, biometrics has heavily moved into the consumer front over the last couple of years with regards to mobile devices, and those authentication capabilities are being used by mobile banking applications and other applications as a two-factor authentication process to help further secure transactions. In addition, as Jessica mentioned earlier, you have groups such as FS-ISAC [Financial Services Information Sharing and Analysis Center] that are using information sharing and reporting in order to disseminate information about different types of fraud, to make others aware of those activities so that they can harden their defenses there.

Chip cards certainly have had a major impact with regard to EMV losses, or counterfeit card losses. Doug wrote a paper earlier this year looking at that activity here in the United States, as well as some activity in some of the foreign countries that are well along with regard to their chip conversion, and signaling some concerns with regard to that.

So with that, we want to kind of put that in the rear view mirror, and move up to slide nine and talk about the changing retail landscape. Doug?

**King:** Absolutely. Thanks, Dave. So I'm all about words and keywords today, going to the fraud slide. But looking at the changes that we saw in 2019—which were really a continuation of the last few years—in my mind those four keywords to note for the year are: digital, contactless, invisible, and mobile. I'll touch on the first three and then turn it over to Dave to spend a little more time on mobile.

But before I touch on those keywords, I do want to mention that the first report from the Federal Reserve's 2019 triennial payments survey was released today—actually released about an hour and 25 minutes ago, I think. So you should be able to find it by clicking on the link to the Federal Reserve's triennial payments survey that is located on the resources slide of this presentation, slide 22. So no need to jump ahead yet, but it's going to be there for you guys afterwards.

But two things that I found compelling and will highlight from the report were the massive increase in the use of EMV chip cards in 2018 compared to 2015, as well as the continued strong growth of remote card transactions compared to the growth of card transactions in general. So the survey found that over half of in-person general purpose card payments in 2018 were chip-authenticated; this compared to 2 percent in the 2015 survey. So clearly that 2015 survey was done right at the time of the liability shift associated with EMV chip cards, and we have seen a substantial increase in their usage.

And then looking at the value of general purpose card transactions in 2018, remote payments value is nearly equal that of in-person payments. Rest assured, the Risk Forum and the industry will have plenty more to discuss with the survey in coming weeks and months. But let's jump back to those keywords, looking at payment trends in 2019, with digital being first.

So our options to exchange money digitally among each other or with businesses continue to expand, as does the number of connected devices that we own and carry. And as these options continue to grow and we become more comfortable using them to send a friend money, or perhaps conduct business at the POS or online, paper-based—and more specifically, cash—payments continue to decline.

Results from this year's Federal Reserve Diary of Consumer Payment Choice saw debit card payments surpass cash payments for the first time in the Diary's five-year history. This year's Federal Reserve Survey of Consumer Payments found that more than 10 percent of consumers have adopted the digital P2P app Venmo. Outside of the Federal Reserve, a study conducted by Square in 2019 found that consumers are using cash in just 37 percent of transactions under $20, and this compared to 45 percent in 2015.

So while the digital era of payments has been here for some time, it's really accelerating as we head out of 2019 and into 2020 with the digitization of lower value payments in full effect.

Contactless: 2019 was a huge year for contactless card issuance in the U.S. Visa has over 100 million contactless cards in the market, and they're targeting 300 million by the end of next year. All new cards from American Express and Discover are now being issued as contactless. Mastercard has commitments from issuers representing approximately two-thirds of its US consumer volume to issue contactless cards within the next two years. And then from a terminal perspective, more than 60 percent of card transactions now occur at a contactless-enabled merchant location.

So I just want to highlight one pilot that was rolled out this year, and that was MTA, the New York Metro's contactless platform pilot, OMNY or OMNY pay. And so they launched this pilot at the very end of May, May 31st, at 16 subway stations, and they had reached one million taps by August. As of today, they have surpassed four million taps, which blew away their expectations that they had.

Earlier this month—I want to say it was maybe this week—they actually rolled out the OMNY pay machines at Penn Station. By the end of the month, or the end of this year, or—this sounds even crazier—the end of the decade, they'll have rolled out the OMNY pay machines at 85 of their 472 subway stations, with the goal of all their stations and buses being supported by the end of 2020.

According to a survey by Visa, they found that New Yorkers' use of contactless payments has increased by almost 10 times in the last year. We've often heard that transit could be the catalyst to contactless payments, and with this MTA pilot and looking at what's going on in the city of New York, that appears to actually be happening here as we exit 2019.

And then with invisible payments, I'm really talking about the continued rise of connected devices and our ability to easily shop through a multitude of these devices. Just looking at the smart speaker landscape alone: according to Pew Research, about a quarter of U.S. adults, which would be about 80 million people, have a smart speaker in their home. In a report that I was reading just this morning, which was detailing a just-announced initiative led by Google, Amazon, and Apple about standardizing connected devices for interoperability, that report noted that smart speakers were in about 30 percent of U.S. households.

So we all know that a lot of people are using smart speakers to play music and look at news, ask what the weather or traffic is before they're leaving, but they are becoming more and more prevalent from a commerce and shopping and payments perspective. eMarketer found that 31 million people will have shopped via smart speaker in 2019, and that's up 32 percent from last year. Further, 21 million people will actually have made a purchase using that smart speaker.

Just a little bit more research from Voicebot. They discovered that of smart speaker users, 26 percent have tried making a purchase, 15 percent use them to make purchases monthly, and 4 percent are using them to make purchases daily. So as people continue to become more comfortable with their speakers for tap beyond those simple everyday tasks, more connected speakers find their ways into our lives. We have faster network speeds coming with 5G. We even have improved enhancements to some of these smart speakers with actual display screens. I think commerce will continue to become more widely adopted, much like with mobile devices.

Speaking of mobile—Dave?

**Washington:** Before you go on, Dave, I just want to say: my son, who is 16 months, his first word pretty much was Google. He doesn't know that you have to say, "Hey, Google," so that's good. And I also wanted to point out that Nacha's Payments Innovation Alliance does have a working group on voice payments, and they're talking very actively about creating standards and security around those voice payments. Sorry.

**Lott:** No, that's great. Just really quickly, and to tag on to what Doug was talking about, slide 10 shows activity since 2013 with regard to online retail sales for Black Friday and Cyber Monday, and you can see that growth. In 2019, Black Friday was the biggest day for mobile shopping, with almost $3 billion in smartphone transactions—61 percent of all the online retail coming from smartphone transactions—and that represents about a 16 percent increase from a year ago, so tremendous growth there.

Kind of on the off side, I was just reading an article this morning with regard to a LexisNexis fraud report saying that they also looked at the activity that occurred on Black Friday and Cyber Monday, and the fraud transactions—that is, those transactions that were identified as probable fraudulent transactions, and denied—the value of those transactions were two and a half times that of the legitimate transactions. So the criminals recognize this shift in activity, and they are moving over in that way as well.

The area of mobile payments and mobile banking is an area of great interest to the Federal Reserve Bank. We conducted a study involving eight of the Federal Reserve districts. They each surveyed the financial institutions in their district with regard to the state of mobile banking and mobile payments. That report—again, there's a link on the resource page—should be published within the next week or so. It's a consolidated report for all of the eight districts there.

But with regard to mobile banking, it really has become a utility service. Ninety-one percent of the financial institutions that responded indicated that they already offered mobile banking, and I think it was another 5 percent indicated that they plan to do so within two years (so it will be reaching up into the high 90s there). Mobile payments certainly has been a little bit less, but as Doug talked about, some of those statistics for this last year—have been growing.

You see on the graph here with regard to the orange showing the mobile payment offerings, which tend to be offered more by the larger financial institutions than the smaller (you have that kind of stair-step down as the asset size of the financial institution decreases there). The smaller institutions are more dependent upon their processors and certainly lack the resources, both in terms of dollars as well as personnel, to operate those things. But we'll see a continued increase in that regard.

Doug talked about the contactless rate. We'll say, as a caveat for this mobile banking survey, that it did not include any of the top 100 financial institutions. So it was heavily focused in on the mid-sized and smaller banks, and credit unions. But they indicated that they did plan to also issue contactless cards within the next couple of years.

And the final point that I would bring out here is with regard to P2P activity. It still remains pretty low based upon the responses that we got, in that more than 70 percent of the respondents that offered a P2P banking service indicated that less than 5 percent of their eligible customers were performing a P2P transaction within the last year. So I think that we'll see that traction improve. It's going to be like mobile payments; it's going to be a slow climb process, but probably at a quicker rate.

So at this point we want to poll you on another question with regard to mobile. Jean, could you pose that question?

**Roark:** You've got it, Dave. Thanks so much. And I just launched that polling question, so I'm going to just pause until it pops up on my participant screen. It's there now, so I'm going to read the question aloud and hopefully you'll grab your mouse and give us a response as well.

The question is: What device did you primarily use to conduct your holiday shopping? So the first option is desktop or laptop computer. Your second option is a tablet, your third option is a mobile phone, and your fourth option is no online shopping. So those are your four options. Let's hear about how you conducted your holiday shopping.

All right, Dave. I see a whole bunch of results still coming in. So we're just going to dance for a few moments here to see if we can get every single response that we can. And they're still coming in, so...all right. They have slowed slightly, so I'm going to go ahead and stop that poll and show the results to both you, Dave, there in the studio in Atlanta, and also to our participants.

So Dave, I'll share with you that 39 percent of our participants chose option A, desktop or laptop computer, and coming in a close second is C, mobile phone. And then 18 percent is tablet, and then 8 percent, no online shopping. So I'll turn it back over to you.

**Lott:** Thanks. Yes, that's pretty consistent with the numbers that we've seen—of course, so much depends upon the item that's being looked at. What we've found is certainly the easy-to-purchase items that are bought frequently, doing that through the phone is easy; whereas things such as clothing and jewelry, people like to have a better look at that, so they tend to skew over to the tablets and the desktop where they can see that a little bit better.

So we've got about 15 minutes or so left, and we want to save some time for questions. So Jessica, talk to us a little bit about faster payments.

**Washington:** Yes, I'll do a quick update here. In August, the Federal Reserve Banks announced they are developing a new interbank 24x7x365 real-time gross settlement service with integrated clearing functionality. That will allow financial institutions to deliver end-to-end faster payment services to their customers, so the pipes are being enhanced.

And so some of the considerations of FedNow are a possible credit transfer system, valued at $25,000 for individual transactions. Settling through the financial institutions' master accounts is a consideration as well. And then also adhering to the ISO 20022 standards, and providing access through FedLine connection.

So please be involved with the request for comments as they come out, or transitioning to opportunities like the U.S. Faster Payments Council—actually, this Federal Reserve just joined as a founding sponsor earlier this month—and so that's a membership organization devoted exclusively to advancing faster payments, and talking about standards and education as well.

I have to mention same-day ACH. The ACH network as a whole has had five consecutive years of adding at least one billion new payments to the system. When we talk about same-day ACH beginning in July 2019, more than one million same-day ACH payments are being processed daily, and so in the third quarter of this year they also saw 54 percent growth. And in March, those same-day payments are going up to $100,000, and that's March 20.

I do want to mention P2P payments. The leaders here in growth are Zelle and Venmo, which might not be a surprise. Zelle even posted a $39 billion volume in the first quarter of this year, which was a 72 percent growth.

And I will point out, the gig economy is booming. Businesses are realizing that paying employees the same day for their work is a competitive advantage. So you'll see, for example, Uber has been very active in ramping up onto the RTP network, the real-time payments network offered by the clearinghouse, and so they've been really taking advantage of faster payments.

And so I'll transition into fintech, and kind of bringing it back home here to the Retail Payments Risk Forum. We have a priority here at the Federal Reserve Bank of Atlanta to make payments safer but to promote innovation at the same time. So we are very engaged with the fintech community, and at the same time we want to work with fintechs to enhance and promote economic mobility and economic resilience. So the slide here is a heat map illustrating economic mobility.

So the defining feature of the American dream is upward mobility. In 1940, a total of 90 percent of children grew up to earn more than their parents, and today only half of children earn more than their parents did. So for us, we are engaging with fintechs and we are identifying fintech innovations, like prepaying your utility bill at a local dollar store, or the ways that Wal-Mart money services are expanding. We're looking for ways that innovations are promoting financial inclusion, but we also want to be careful to identify if payment innovations may be excluding some populations.

So there'll be more to come from our group on that topic, but we absolutely want to engage with the industry around this topic.

**Lott:** Certainly the world of fintech, with regard to mergers and acquisitions, has been very hot in 2019. Three of the four top fintech acquisition deals have involved payment-related companies. You see on the slide here those three big ones, but there certainly have been others involved. Mastercard and Visa both have been very heavily involved in terms of looking at opportunities to engage more of the fintech community.

You see on this slide, on number 15, with regard to the M&A activity, the blue column showing fintech as a whole, whereas the orange is the payments side of things. You can see in 2019, the number of activities is lower than 2018, but certainly the dollar value is higher and the payment side of those acquisitions has a greater share of the overall fintech activity. So that will continue, we think, in 2020.

Related to fintech—and Doug and Jessica made me put this toward the end because they knew I'd go on my rant if we had it on the front end, but—is this evolution towards AI. I was at a conference last week in New York, the AI Summit, that brought together more than 5,000 attendees to look at all the different applications of what is called AI, not only in financial services but in healthcare and other industries as well.

My rant is that there's not really any true AI today by the pure definition of it. We certainly have the increased computing capability with regard to the evolution from neural networks to machine learning and deep learning, and that development is highly active and will continue. But it doesn't come without risks, as shown on slide number 17.

I was at another conference, a federal government conference with regard to biometrics, and there was concern and a speech by an academic person who made the statement that [with] some of the deep learning algorithms, there would be no way that a human could validate the results that that deep learning algorithm came out with. Certainly from a regulatory compliance standpoint, that creates a concern. Jessica and Doug talked about data breaches and things of that nature, so garbage in, garbage out. You have to make sure your data is good, it's stored safely, and it's accurate. You have to protect the algorithms from the potential for bias, or illegal use and noncompliant use.

Processing power: we could do a whole webinar with regard to quantum computing and what that's going to entail in the future years and the risks that are posed there. So, talk to me later about AI. *[laughs]*

Doug, how about some discussion about some of the nonfinancial institutions' involvement?

**King:** Yes, there's no doubt 2019 can be highlighted by some major announcements from some, we'll call them high tech players. Perhaps Wall Street calls them "FAANGs" from a stock performance perspective. But Apple, Google and Facebook all made major announcements and have major things going on in the payments space. I think the really interesting thing to note, or the key takeaway for me with these announcements, is that they're not trying to go at this alone. They're either partnering with traditional financial services or institutions, or perhaps partnering with more established alternative payment providers.

How they're going about that is definitely different. We've seen with the Apple Card, they're trying to distance themselves and present that product as a financial institution product, while Google and Facebook I think are making it perfectly clear that "we're in this with payment providers or traditional financial service providers, and truly in a partnership role."

You'll notice Amazon is not included on this slide, but they have definitely been highly active. So if you look to slide 19—I'm not going to go into detail on this slide, but I just wanted to include this great graphic from CB Insights just to highlight that as a nontraditional player, they're doing more than just biting or nibbling around banking and payments, but are really jumping fully in with a host of products and services that really mimic those offered by financial institutions.

And within all this activity, you'll see—as we get to slide 20—things involving payments and financial services have been pretty sleepy on the Hill and in the courtrooms for several years, outside of the seemingly always-ongoing litigation around payment card interchange fees and merchant discount antitrust litigation.

But this really changed in 2019. And I think hot for 2019, when you talk about Washington and DC, was with the Libra Association. A lot of discussion around stable coins, digital currencies, cryptocurrencies, and shortly after the Libra Association announced the intentions of launching this digital global stable coin, Libra, Congress took notice and a hearing was held on Capitol Hill, where it seemed to be pretty apparent that most lawmakers were highly skeptical of the venture from a regulatory standpoint as well as a data privacy standpoint.

So I think it leaves us with: there are some headwinds, it appears, from a legislative perspective; and then, will these headwinds influence any regulatory decisions related to this whole stable coin and cryptocurrency situation?

One other area that was touched on and has been on the Hill for several years, but not much is being done, is related to data privacy.

**Lott:** Yes. You know, it's going to be interesting to see what happens here. There's been a lot of discussion but very little traction over the years with regard to privacy and data rights legislation, certainly in the EU with the GDPR that went into effect that has prompted more pressure here in the United States. You had the state of California, with their Consumer Privacy Act that's going to go into effect in early 2020 that is patterned to a large degree after GDPR with regard to consumer rights to understand what data is being collected, how it's being used, and to make sure that it's being used for the purposes to which the consumer agreed.

There's a number of states with regard to data breach notification laws, and it remains to be seen whether or not there's going to be federal legislation to try and simplify that, to have that common to all the states rather than individual states there. So on slide 22, as Doug mentioned earlier, we've got a resource page with these links to the Risk Forum as well as some of these studies that are done.

We've got about five minutes left for your questions. You've heard our perspectives on key events and issues, and so we wanted to see if there is something that we missed from your perspective, or something that you would ask us to discuss a little bit more.

Jessica, have we got some questions here?

**Washington:** Yes; we have two questions that I'll pose to the group. Most of the fintech acquisitions and partnerships are taking place involving the larger financial institutions. How are the small and mid-sized FIs going to compete?

**Lott:** I would say that it's going to follow along what I pointed out with regard to mobile payment services. The smaller institutions are highly dependent upon their processors—in this case not just their core processors, but other third-party processors—to provide those services because they don't have the financial and the human resources available to attack these issues like the large financial institutions do.

Doug?

**King:** I think it's a great question, and they're definitely going to be challenged. But I think they're not going to become dinosaurs; they can play in this new world. I think of real-time payments in the clearinghouse; there were a lot of people who thought that was only going to be for the large banks, and I think we've seen during this year 2019

that a lot of smaller institutions have been able to become a part of that network and participate in that network.

Is it easy for these guys? Definitely not, because they don't have the resources of the larger ones. They don't have the staff, they don't have the capital perhaps. But I don't think they're going to be left in the dust per se, unless they choose to do so.

**Washington:** And we see more cloud-based core processors creeping up and making impacts on the market, and I think that being nimble will be important as we go into that digital world.

**King:** And I think you'll continue to see consolidation within that space as well with those small or medium-sized financial institutions.

**Washington:** So the next question is: You mentioned a number of regulatory and legislative issues. What do you think is the most important?

**King:** I think data breach and data privacy. We've seen those continue to proliferate year after year, and nothing being done at the federal level—which makes it challenging for those consumers or victims who have their information compromised and makes it difficult for those businesses who have a web of reporting requirements, or difficult to say, "How do we unwind from this?"

**Washington:** I would say I agree with you. I think probably privacy right now is most important. But I do want to mention the OCC fintech charter, and any place we can move forward, because the definitions of all these participants in payments, in fintech, have changed so much to base our regulatory system on, where stakeholders are now just completely different entities. So it's hard to apply certain regulations based on those changing entities' structures.

**Lott:** Thank you. That's all the time that we have for questions. Jean, do you want to close us out?

**Roark:** Yes, that'd be great. Thanks so much. I am going to push the survey out, so you guys should see a link pop up for you. I'd like to thank our presenters today, Jessica, Dave, and Doug, for sharing your time and expertise with us. And as I mentioned, that survey is now available for those who have joined us via webinar, and shortly everyone will receive this same link via email. You only need to fill it out once, but please do take just a couple of minutes to give us your feedback.

Thank you so much for joining us. This concludes today's *Talk About Payments* webinar. Enjoy the rest of your day.

View previous *Talk About Payments* webinars on our website.

**RELATED LINKS:** Play (MP3) • • Presentation • *Talk About Payments:* Cash in the 21st Century • *Talk About Payments:* At the Intersection of Fintech and Financial Inclusion • *Talk About Payments:* Bridging the Fintech Talent Gap