



Changes in US Payments Fraud 2012–16 Transcript

November 1, 2018

Brad Straubinger: Good afternoon, and welcome to the Federal Reserve Bank of Atlanta's Talk About Payments Webinar: Changes in U.S. Payments Fraud 2012-2016. I'm Brad Straubinger, from the Center for Learning and Innovation at the St. Louis Federal Reserve, and I'll be your moderator today. We are joined by Mary Kepler, senior VP and chief risk and compliance officer from the Federal Reserve Bank of Atlanta; Geoffrey Gerdes, principle economist in payments systems studies from the Board of Governors; and Claire Greene, payments risk expert in the Retail Payments Risk Forum from the Federal Reserve Bank of Atlanta.

I want to run through some logistics real fast for you, before we get going here. If you have not had a chance to join us in the webinar, please click the link provided to you in the webinar invitation. Please note this call is being recorded, and everyone's phone lines have been muted.

We will be pausing for questions at a few points in the conversation, so at any time if you do have questions, you can simply email us at rapid@stls.frb.org—that's rapid@stls.frb.org—or you can simply just click the "Ask Question" button in the webinar and type your question there, and we'll get it to our presenters.

At this time, I'll go ahead and move to slide three, and turn it over to our presenters.

Claire Greene: Hi, this is Claire Greene; thanks for joining us today at the webinar. We're here with Mary Kepler, the executive sponsor of the Federal Reserve Payments Study, and Geoff Gerdes, a principle author, along with May Liu.

Now I'm moving to the next slide, please; slide four. In today's conversation, we will be talking about three large topics: First, an overview of the data environment and scope for the study...I beg your pardon, this is slide five.

And then second, a review of the 2012-2015 data from surveys of depository institutions in the U.S.; and third, a review of 2015 and 2016 data resulting from a survey of U.S. card networks.

So now, on slide six, I'm going to turn it over to Geoff to give a quick overview of the key findings of this report.

Geoffrey Gerdes: Good morning, everyone. So, this study, we figured it'd be a good idea to give you an overview before we get into the details. What we found was that the overall rate of payments fraud increased from 2012 to 2015 in the United States. The share of card fraud by value increased from less than two-thirds to more than three-quarters over that time period, while the shares of ACH and check fraud each declined.

The rate of card fraud, even though it's the highest, is still well below two-tenths of one percent of card payments. The rate of card fraud by value had checked its rise from 2015 to 2016, and actually dipped slightly—although not significantly, so it kind of had a flattened-out period during that time, and we'll get into the details as to why. But the stabilization is due to a decline of in-person, counterfeit-based card fraud, and that in turn was driven by a sharp increase in microchip-based payments. Remote fraud, conversely, increased as the remaining categories of card fraud, besides the counterfeit-card category, were rising over that one-year time period.

Card fraud from 2015 to 2016 showed a slight decline from 13.55 basis points to 13.46 basis points. We'll show you that detail later.

Greene: So, quickly on slide seven, before we get into more on the data we're going to ask three questions, and that's why we study payments fraud; give you an overview of the data used for this analysis; and then define third-party payments fraud as it's discussed in this report.

So, on slide eight I'm going to turn it over to Mary Kepler and ask the question: Why is it important to study payments fraud?

Mary Kepler: Well, an efficient, effective, and safe United States and global payment and settlement system is really vital to the U.S. economy, and the Federal Reserve plays an important role in helping maintain that system's integrity through operating and overseeing the nation's payments system. So quantitative data is needed to inform policy and decision making—in fact, these fraud data give the Federal Reserve, the financial industry, public policymakers, and anybody else who's interested the information that can help inform prevention and detection of payments fraud. And until now, this degree of detail about payments fraud from an unbiased data source has been unavailable, so we're really excited to be sharing these results.

Greene: Now we'll turn to slide nine, and just report on the data source for this report, which is the Federal Reserve Payments Study. So since 2000, the Federal Reserve Payments Study has tracked the aggregate number and value of noncash payments made by U.S. consumers and businesses. And beginning with the year 2012, the Payments Study has collected data about fraud.

So as you can see on the slide, the noncash payment instruments included in the study are cards, ACH payments, checks, and wires. For purposes of this report, we will be excluding wires from the conversation, and for cards, we're talking about general purpose cards. The economic actors covered include government, business, and consumers, and the respondents to two separate surveys have provided the data for this report. The data we're discussing today is from 2012 and 2015 surveys of depository institutions—that's banks, saving institutions, and credit unions—and then, from 2015 and 2016 surveys of the card networks.

So, turning to slide 10, you can see in the purple boxes what types of payments are defined as payments fraud in this study, and I'm going to turn it over to Geoff to describe what's included.

Gerdes: Well, if you look at the chart, you can see a web of dispositions for cleared and settled fraud payment transactions, and our study covers all of those. It is not designed to measure costs, for example, or underlying costs; it is just covering transactions as they are cleared and settled. So, for example, attempts at fraud would not be included in the study, if they don't clear or they don't settle through and don't actually result in a funds transfer.

On the other hand, even if a fraud has settled in a funds transfer, it is possible for various parties to recover what could have been a loss to them; that detailed look at what happens to fraud once a third party breaks into the payments system is really out of scope for this study.

Greene: So before we move ahead, just a reminder about what's outside scope, and that includes the cost of prevention, mitigation, and also any information about ID theft or data breaches, because while ID theft and data breaches may eventually enable payments fraud, they do not necessarily involve an unauthorized payment.

Now, starting with slide 11, we're going to take a deeper dive into the detail from the 2012 and 2015 surveys of depository institutions, reporting on third-party fraud in ACH transfers, checks, and card payments.

And on slide 12, I'll turn it over to Mary.

Kepler: All right. So, this slide focuses on just fraud in general, and the value of fraudulent noncash payments in the United States rose significantly between 2012 and 2015, outpacing the growth in noncash payments overall. Fraud rose 37 percent, while noncash payments rose 12 percent. So, that's really the context for this conversation; and Geoff, I'd like for you to talk a bit about why both value and number are important when we're looking at fraud.

Gerdess: Well, so we do look at both value and number, and in fact we do that for payments overall. But for fraud specifically, value is important because it represents actual financial amounts at risk, and so that sort of affects people's bottom line. The count of fraud transactions may not matter for loss purposes but certainly relates to the amount of incidents that are supporting the amount of value potentially being taken out of the payments system by fraud perpetrators.

And before going on, I want to point out: So this slide shows that both number and value of fraud are increasing, and this is in a background where the payments system itself has been exhibiting extremely high growth. So, looking at increases in fraud by themselves is not really going to give you a good sense of to what extent the system itself is at risk, given that there's so much growth in noncash payments. We need to be able to address that using other statistics.

Kepler: That takes us to slide 13, which is about fraud rates. The 2015 payments fraud rate by value was more than 20 percent larger than it was in 2012, while the 2015 fraud rate by number was nearly 70 percent larger than in 2012.

So Geoff, this is the first slide where we show fraud rates, and that's a common method of comparison that we will continue to use throughout the presentation, so please talk about why the fraud rate is important to measure.

Gerdess: OK. Well, slide 13 shows these rates by value and by number; and on the left you see the 2012 and the 2015 fraud rates at .38 basis points in 2012 and .46 basis points in 2015. So what this is showing is that the rate of fraud did increase a bit. Even though payments overall were increasing, because the rate has increased, that means that the value of fraud increased faster than the value of total payments.

And then, on the right you'll see the fraud rate by number—that's 2.6 basis points in 2012 and 4.38 basis points in 2015. And of course, that also is a large rise.

Now, relating the two: Obviously, by value the rate is much lower than the rate by number, and this has something to do with the underlying data. This is aggregate cards, ACH and check data that we're looking at here, and check and ACH systems support extremely large values, so the denominator in this ratio will affect...what that says is that large-value payments may not be as high of a risk of fraud as smaller-value payments.

And also, just to elaborate on what basis points are—because it's easy to, if you're not using basis points every day, to not quite understand what the magnitude of these are. So if you look at .46 basis points by value in 2015, what that is, is roughly 50 cents on \$10,000, because a basis point is really one one-hundredth of 1 percent, so it's a very small number. Again, when we saw the totals before we looked at the rates, these numbers are in billions of dollars; so we don't want to take away from that fact, but the payments system itself has a very large value going through it, so as a rate it's much lower.

Greene: Another thing that we see on this slide is change from 2012 to 2015, so perhaps this is a good time to ask: Can you use this data to say something about trends?

Gerdess: Well, clearly we have to say this is showing that payments fraud appears to be on the rise, but whether these are long-run trends or if they're short-run trends remains to be seen; and I think we'll see as we go into the details there are very specific events that have affected fraud in recent years, and will probably continue to affect fraud. So this is a change, it's an increase, but we're not clear on whether it means there will be increases or decreases in the future.

Kepler: All right. Go to slide 14—and Geoff, we're going to go back to this idea of the basis point and very small amount of fraud, and why is that meaningful; but as you can see here, fraud is a very small fraction of payments value. There was an estimated 46 cents of payments fraud for every \$10,000 in payments in 2015, compared to 38 cents of payments fraud for every \$10,000 of payments in 2012. But Geoff, talk about why these very small amounts still matter.

Gerdess: Yes. Well, so, I did get ahead of myself, and I don't think I mentioned this before, but ... this slide really emphasizes the tininess of fraud; but at the same time, the loss affects different types of payments differently, and as we'll see looking at card fraud, for example, individuals or banks that issue cards may be more concerned about the amount of fraud that may be going through cards than through some of these other systems. Nonetheless, if you look at ACH or check, you may be more concerned about certain segments of those markets, and where fraud may be coming through those markets.

So, again: Overall, the Federal Reserve System is not at all unhappy about being able to report overall things are quite...the rate is quite low, but at the same time we have to recognize it's very important that every segment be watched closely, and that fraud needs to be monitored carefully. Because it is large losses when you look at them in general.

Kepler: All right, so move to slide 15; and this slide shows how fraud by value is distributed among the different payment instruments, and most of the payments fraud is by card. So by value in 2015, 77.5 percent of payments fraud was card fraud. By number, in 2015, almost 98 percent of payments fraud was card fraud.

So Geoff, can you talk a bit about the change in the value of card fraud from 2012 to 2015?

Gerdes: Yes, well, from 2012 to 2015 card fraud increased at a rate that was basically three times faster than the rate of payment transactions by card; and by value—just to reiterate what we said before—it accounted for more than three-quarters of noncash payments fraud in 2015. This is up from less than two-thirds of the fraud pie in 2012.

Greene: So moving to slide 16 and following up on the prevalence of card fraud, you can see here a comparison of the rates by value and number in 2015 for card fraud compared to ACH and check fraud.

Gerdes: Well, so the rates tell a similar story to what we just saw when we looked at fractions of total. By value, we looked on the left of the slide and ACH fraud is really .08 of a basis point, which is really a tiny fraction of a tiny fraction. And check fraud was higher than ACH fraud, but this is by value, and partly that has to do with the fact that ACH is transferring very large payments relative to check.

And then you look at card, and you see that, in basis points, we've got 10.8 basis points; and that's much higher of a rate. So, it tells you where you should be looking out for fraud. By number, the story is very similar: Card fraud is just sort of overwhelming the amount of fraud in ACH and check; and you see there, by number, the rates of fraud between ACH and check are quite comparable.

Kepler: So, on slide 17 we start to focus on card fraud. There are two things on this slide; first of all, credit has consistently higher rates of fraud. The ATM, which requires PIN authorization, is the lowest rate, as you might expect. But note the growth in rates for all types of cards; the card fraud rate is up overall by 40 percent.

So Geoff, what do you make of this?

Gerdes: Yes; so this is saying that fraud is increasing across the board, by different types. And Mary, you mentioned the PIN; PIN access, if you have a PIN-protected card but, as a fraudster, if you have access to the PIN, you might want to go straight to the ATM. That may be a rare event relative to other opportunities for fraud with cards, and that often might be where you would end up going, just because that's a very liquid opportunity for theft.

And you look at debit cards: Debit cards tend to be used more at the point of sale relative to credit cards, which often are used for... people might have more confidence to use credit cards in a remote setting, for example. And so you see, for debit cards, you see that fraud rate is combining PIN-based payments as well as the no-PIN kinds of payments that you are typically seeing with credit cards. So it averages out to a lower rate in that sense.

Kepler: So move to slide 18, and we'll focus on ACH fraud. So this slide shows that ACH credit transfers originated by the payer's bank appear to be less subject to fraud than ACH debit transfers, which are originated by the payee's bank. The fraud rate by value of ACH credits in both 2015 and 2016 was less than half the rate of ACH debit transfers. So as you can see, these rates generally declined from 2012 to 2015.

So Geoff, can you talk about the decline in ACH credit rates by numbers? Given that these rates are so small—about half of a basis point—how should we think about that?

Gerdes: Well, by value the rate was pretty steady for ACH credit transfers—which, by the way, I'll point out were less than half the rate of ACH debit transfers; but by number, you see that there is a fairly significant decline. And we don't really know what's behind that; I think those that are in the business may have some ideas, but sort of a simple, descriptive explanation might be that it essentially means that the average value of ACH credit fraud has increased over time, per fraud, but a fixed total amount of fraud coming out.

But you also see the same decline by number in ACH debit transfers, so I think there's just perhaps more attention being paid over time to high-value transfers, and different opportunities that are available. It's really hard to say, because this really comes down to a competition between those preventing fraud and those trying to break into accounts, and I think you're going to see some volatility in there.

Kepler: Now, our slide doesn't have any information on it about check fraud, but check fraud still exists. So, what about check fraud; what happened there?

Gerdes: Well, yes it's true (that) by number, checks declined over the past three or four years. What we've seen is that by value actually, check as a total number of check payments, the value of check payments increased over that time period...which is not that well understood, but it really has to do with more emphasis on business payments over time, and greater value business checks being written. That really has to do with the underlying real economy than it has to do with the payments system. And then, as a result you see the value, the rate of check fraud, declining over time.

But also, in fact, the total value of check fraud declined as well; so check fraud tends to have a similar average value for checks, whereas for cards and ACH, usually the fraud payments will average out to something different than what a normal payment would look like, but for checks it seems that the kind of fraud that's going through checks is just a little bit different. But it is declining.

Kepler: All right. On slide 19 we're going to move back to card fraud, and in fact the payment channel, which is characterized in terms of the physical presence of a card or cardholder; and this characterization does influence the opportunity to commit payments fraud.

So this chart shows fraud shares by number and value for "card not present" and "card present" payments. As you can see, the share of fraudulent payments that are "card not present" exceeds the share of all payments that are "card not present" both by number and by value.

So Geoff, do you want to talk about the value relationship being closer than the number relationship?

Gerdes: Well, yes; so the value relationship being closer, it's still higher. So fraud is higher, there's just more opportunity in a "card not present" situation for fraud, and as the population may be ... as regular, legitimate payments are being made more frequently in a "card not present" situation, it's just a more attractive environment for fraud.

That's one reason why, and it's just the types of payments that underlie the two, either "card not present" or "card present" payments, are different. "Card not present" includes online payments, telephone catalog kinds of purchases. It also includes bill payments, and so when you look at bill payments, they tend to be rather high value payments, for example. But also not necessarily as risky as other types of payments, because if one is paying a utility, it's less likely to be an opportunity for fraud.

Kepler: All right. Let's go to slide 20, and talk a little bit about the PIN, the use of the PIN. So for "card present" transactions, activity that involved the PIN has generally been regarded as a more secure activity than without a PIN, because the former requires the cardholder to enter an additional authentication factor at a terminal. So let's talk a little bit about what happens with fraud when the PIN is used.

Gerdas: OK. Well, PIN-protected payments, as a fraction of all in-person payments, or legitimate payments, are still less than half of those payments. People are finding payments without PINs to be quite convenient, and they're encouraged to do so. And over time that's where a lot of the growth in debit card payments has been—is in payments without the PIN.

But nonetheless, the patterns show that PIN-protected payments are not nearly as likely to be subject to fraud. And so, it makes you think, "Well, if PIN is being used less, will there be ways of replacing the protection that is provided by PIN, or is it necessary?" It's certainly a conversation we need to have. But we'll also talk about chip payments—that's a new, modern way of protecting certain things that PIN was used to protect but may exhibit a different sort of fraud profile than PIN.

Greene: So that sums up the quick summary of the results from the 2012 and 2015 surveys of depository institutions. If you go online at federalreserve.gov you can see the complete report; and also, many of the charts we're showing here today are simplifications of more detailed charts that you can review in the report.

Next on slide 21, we'll move ahead to the 2015-2016 survey of the card networks. So I'll turn it over to Mary to talk a little bit about categories of card fraud, methods of fraud.

Kepler: All right. So we're on slide 22, and this slide shows that in 2015, fraudulent use of account number is the most common type by number, but counterfeit card is the most common type by value. So the value relationship changed in 2016, with fraudulent use of account number most common by both number and by value.

So Geoff, talk to us a bit about the change here.

Gerdas: Well, so counterfeit fraud, as we said before, was the only category that fell, and we believe it's connected to this sharp increase in the use of chips for payment in an in-person situation, which we've also seen be basically driven—most of us who use cards know that you're often asked to insert your card into the terminal instead of basically swipe the magnetic stripe, and that change has made it harder...at least, as merchants adopt this technology and ask people, and as these cards are issued, there's less and less of an opportunity to counterfeit a card. The chip does a great job of preventing...at least, so far with current technology it's just not something that can be counterfeited.

Essentially, you could say this has pushed those that want to commit fraud to need to look to other opportunities, and that has been every other category. So I'd like to say one thing about, now that we're talking about the network study, we collected data in 2015 not only from the depository institutions that we reported last time but also in 2015 also from the card networks.

And now we're looking at the change, just looking at the card networks. There are some differences. The surveys are consistent but we've presented them in the report separately, and then there's an analysis at the end that explains where the differences are. But ultimately it tells a consistent story, and the card networks have this kind of data where they have historically tracked these different categories. So, lost or stolen, for example: You know, a chip card, the chip does not protect a card from being lost or stolen in the way that it can prevent a card from being counterfeited, and that's why we don't see lost or stolen declining when it comes to chip cards, for example.

And that's the same thing for remote payment, you can still use it the same way one did in 2015, they use it the same way in 2016. Of course, you know, people are trying to roll out ways of protecting remote card payments as well, but at least for this time period, there seemed to be a very clear shift.

Kepler: So, slide 23 actually shows a little bit more of what you were just explaining, Geoff. In-person card fraud decreased from 3.7 billion in 2015 to 2.9 billion in 2016, while remote-card fraud grew from 3.4 billion to 4.6 billion. Those are meaningful increases, and you can see in the slide that the rate of remote fraud by value increased while the rate of in-person fraud value decreased. Any other thoughts about the shifting of the fraud channel?

Gerdas: Well, we've discussed some of that already, but what I will say here is that now what we're seeing is really the highest fraud rates overall are coming from card payments in a remote setting, so this is where we would expect people to want to pay attention.

Slide 24: So this is just relating to that sharp increase in chip use at the point of sale, and so by number we had a very small portion—really, 2 percent of in-person card payments were made using chips... a lot of us are thinking about EMV now, but this includes contactless payments as well as mobile payments, so mobile and contactless. Chip payments we've been tracking for a number of years, and they've exhibited pretty strong growth in terms of rates, but of course, as you can see here by 2015, they were still such a small fraction of total payments by number—and by value, it was 3 percent in 2015.

And then you see this very huge jump, really, in 2016. So this essentially supports the argument that this had a lot to do with that decline in counterfeit fraud.

On slide 25: So, what we've seen is that the remote card channel has been increasingly popular for shopping and other payment situations, and we've seen steady growth over multiple cycles. From 2015 to 2016, we saw that all remote payments—basically, the legitimate remote payments—just from year to year grew 11.1 percent over that one-year period, which is a pretty decent growth rate for a single year. But as you also see in the slide, remote fraud grew substantially more—three times more.

Kepler: So you can see here, just by these numbers, that remote fraud is likely to be of increasing concern. And going forward, the Federal Reserve Payments Study will continue to collect fraud data in order to determine whether or not these particular changes foreshadow any persistent trends.

Gerdas: On slide 26, just to sum up—and we've reiterated this—we have a great deal of data in the report, and it's a fairly lengthy report. It has an executive summary that gives more detail even than we've discussed here. And then if you have a taste for it, you can dive into much deeper discussions in separate presentations on the two surveys, where you can look into those details.

But what we see is that the overall picture is fraud has been rising. We want to continue to collect data in order to be sure of where the trends are going, I think, and it's to continue to monitor the situation. We're going to continue to collect fraud data and report information out as analysis is completed.

OK. Well, so now we move to the questions and discussion section, on page 27, and we have received a question. It says: Given that the implementation of strong authentication—EMV—addressed "card present" fraud, what does the Federal Reserve anticipate will happen to introduce strong authentication for other types of payments?

Well, that's a good question; I don't think that I would be able to answer that myself. I would say, over time we've seen that if fraud is a cost to businesses, they're going to find a way to solve the problem. And Mary, do you have any thoughts about what we're doing in the System to address fraud?

Kepler: Well, we have several efforts under way across the Federal Reserve System to quantify fraud, that provides information for investment purposes, for organizations whether it's merchants or financial institutions, to make decisions about whether or not this increase in fraud warrants some kind of response, investment response, to prevent or detect the fraud. One of those efforts also focuses on understanding fraud mitigation that goes on in financial institutions or merchants, corporations, so the Federal Reserve will probably continue that work. Again, it's to generate information so that users can make decisions, use that information in making decisions about making investments and mitigating fraud.

Gerdess: I would say that our study has benefitted from the fact that the card networks were already set up and for many years were tracking fraud types. And I'd say that, given that fraud is shifting, perhaps the card networks will be looking toward maybe collecting information reported by new categories that address the kinds of fraud that may be coming through in more recent times and maybe anticipating where fraud might be going, it might be worthwhile considering new categories.

But not to complain about the card networks' efforts, because when you look at it, I think that the other payment types haven't had as much of a promotion by...if you look at ACH and check, there's not quite as much information about fraud in the public space. And whether check is declining, it's not clear that that's where efforts will go unless fraud becomes a serious problem there. In ACH, I think that there are efforts out there to develop better measures of fraud going forward as well.

Greene: Brad, are there any other questions you'd like to ask?

Straubinger: Yes, we had a few come in: Do you consider any of these results to be surprising?

Kepler: Well, we used the data that we have to understand...

Greene: Sorry; he said, "Do you consider any of these results to be surprising?"

Kepler: Oh, "surprising." Yes, I'm sorry; OK. I heard "spreading." [laughter] All right; "surprising." Well, yes; actually, I was surprised by the overall amount of fraud, and just how small it is.

Gerdess: Well—this is Geoff—and it being detail-oriented, I was initially surprised—and you'll find this in the report, we didn't emphasize it here—but the fraud rate for chip cards jumped in 2015; it was quite high relative to nonchip fraud in the in-person setting, and that seems counterintuitive. It doesn't really necessarily say anything about the adoption of chips per se, but rather maybe the way that the statistics came in for that year, because basically the card terminal acceptance of EMV started to be rolled out in the last two months of the year, and so the rate is essentially being calculated on a very small number of payments.

And there are probably other surprises, but I think we shouldn't go rattle off a laundry list of them.

Kepler: Well, at the same time, there are a lot of results that were probably as expected.

Gerdess: Yes.

Straubinger: Yes, we have another one here: What is planned for future releases of FRPS fraud data?

Gerdess: Well, just to define "FRPS," that's the acronym we use for our study, the Federal Reserve Payments Study. Yes, at this point, I think we're interested in continuing to measure things as we have, as well as work with industry and others to look for new ways that we might be able to measure things. And we'll report things out as the data become available; ...sometimes it's not easy to roll it out right away because we've got to do follow up—and that's one of the benefits of our study, and why we feel so confident in our results is because of the effort we go to (to) validate the data that we receive and make sure that the messages that come out are accurate. And we hope to release information as timely as we can.

Kepler: Well, and we are collecting fraud data in the annual supplements that we're looking at right now, and we'll be collecting fraud data as part of the triennial study which will kick off next year.

Gerdess: And, to be very specific about this year: It's unlikely we'll have any more fraud data to report this year, but we will be reporting things likely next year sometime, but it's not clear to us exactly when that will occur yet.

Straubinger: All right, we had another one come in here: With strong authentication techniques like WebAuthn, biometrics, multifactor authentication, any chance the government will ask the Fed to look at, and introduce, strong authentication? Clearly faster payments saw strong authentication as a key issue.

Kepler: Well, that's a good question, and I can't predict what the government would ask the Federal Reserve to step in and support or do. Some of these strong authentication efforts, they come from the market, and they are designed to address issues like this, and I would anticipate that we'll let the market continue to produce solutions like that.

Gerdess: Yes. As we look at the System, it's fair to say that fraud is fairly well contained in an overall sense, and as is the tradition in this country, the Fed has typically looked to industry and supported the industry in ways that we can be effective given our role as mandated by Congress.

Straubinger: All right, and another question that came in: Can I compare the two types of 2015 data—some from networks, some from depository institutions?

Gerdes: Yes, you can compare them. So I will say that there are differences, and in the report there actually is a section in the appendix. The first appendix is describing how the data were collected from the two, and then how the numbers differ. And what we learned was that the card network data was suggesting higher fraud rates for the general purpose cards than the depository institutions survey. Partly that could be related to estimation techniques, whereas the card networks are essentially aggregated from the total reported by the networks. What we found there was the credit card rates were higher as reported by the card networks than they were in the depository institutions study.

Now, for debit cards, the regional networks have not all been able to do an excellent job of tracking fraud on their own networks because of the kind of role that they play. They don't necessarily stand in between, and require the reporting of fraud in the way that the more prominent network brands do—and for that reason, we need to look at the two surveys together, because you get the perspective of the issuers from the depository institutions study. Nonetheless, the estimates for debit card were much closer than they were for credit.

So, what's the reason for that? It's really not for us to say why would it be higher as reported by the card networks for credit cards, and I think it may have to do with the scope of information that they have, and a variety of other things. And I think as we move forward, we'll have more clarity on that as we collect data and analyze it over time.

Straubinger: All right, and had another question that came in: What else is the Fed doing to examine payments fraud?

Kepler: Well, there are several complementary methods under way to examine fraud, fraud prevention and also fraud mitigation. Those include the SPS, or Secure Payment Strategy, through which the Fed is leading collaborative efforts with the industry to examine and mitigate payments fraud. There are also surveys by Federal Reserve Bank of Minneapolis; and I mentioned these earlier, these are surveys that collect the qualitative information about the way banks and merchants address fraud.

Also, we have surveys by the Federal Reserve Bank of Atlanta that ask a nationally representative sample of consumers about their experience with payments fraud. So, you can see we're trying to get the information from several different perspectives when it comes to fraud.

And then, finally, there are debit issuers' fraud report information that is required by Reg II. So, just several different ways of gathering information or perspectives on payments fraud.

Straubinger: All right, and at this time, I don't see any other questions in, so I'll give folks one last chance if they do have a question to go ahead and type it in. You can hit the "Ask Question" button in the webinar tool, and go ahead and send us one through that, or you can email us at rapid@stls.frb.org.

At this point, I'm not seeing any questions come in either way—actually, we have one that just came in here kind of rapidly. So I'll read this, and if you guys can answer it, I'll let you go ahead; if not, you can take it online: With the paper coming out of the Better Identity Coalition addressed to Congress, the work done by NIST on things like 800-63-3, and the concerns surrounding cybersecurity becoming a worrying national concern, both from a national security and simple economics perspective, one would expect activity in the digital identity and authentication space. How can we help?

Gerdes: Well, so I'm going to speak. I'm the least likely to know the answer to that question as a survey researcher, however...so what we feel our role is, is to help document these kinds of changes, and as we work with the industry to find out what kinds of survey questions we could ask, we'll be going out with a request for comment on our new surveys and we would appreciate any kind of suggestions or support you have on how we could track this better. Because sometimes we realize that there are things that are very important for policy reasons but aren't always that easy for our respondents to report, or could cause a lot of burden.

So we have to weigh the burden of conducting our data collections against the importance of the policies; because we cannot do this alone, it's a partnership, and we have to...and so, but in that sense, we do want to hear the kind of feedback, what kinds of things would the industry like to see out of our study, and what could we be measuring to help contribute in the future.

Kepler: So Geoff, that was a really effective way to take the question and turn it back around to, "How can we help?"

Gerdes: Yes.

Kepler: So we're looking for input.

Gerdes: Yes. Are there any more questions?

Straubinger: Yes, we have one more here, and I'll go ahead and ask this and then we'll wrap: What does the Federal Reserve see as its role regarding fraud for the broader FS industry? As an example, is the Fed looking to drive R&D innovation as it relates to fraud detection innovation through items such as AML-based fraud? Or is the Fed, in this study, purely informational to inform the broader community?

Kepler: Yes. The answer to that is, with this particular study and the work we do around fraud, it's really to inform, provide the data on fraud that would inform decisions about what to do about fraud. So we're not looking to drive any particular solution, or technology, or choose some winning approach to combatting fraud but rather want to supply the information that just gives people a baseline to understand where fraud stands, and then move forward with how to deal with it.

Gerdes: Right. We're kind of, since we're dependent on the survey responses, we're essentially dealing with being able to report historical data, and we hope that that helps the industry anticipate what they might do in the future as...you know, and to input, it's important to study the past, as we all know.

Straubinger: All right, well I don't see any other questions, so at this time I'll go ahead and ask our presenters if you guys have any final thoughts before we close out today's session?


Gerdes: Thank you for your interest, and please go to our website, which probably is...

Greene: If you go to federalreserve.gov, you'll find it, and there's also a link in this slide.

Gerdes: Yes. And click on "Payments Systems" at the federalreserve.gov website. You'll see a splash page about our study, and you can get lots of information there.

Straubinger: All right. Well, at this time I'd like to thank Mary, Geoffrey, and Claire for sharing their time and expertise with us. In just a few minutes, you'll receive a survey link via email; please take a few minutes to complete that and let us know how we're doing.

Thank you for joining us today; that'll conclude today's webinar. Have a great day.

RELATED LINKS: [Play \(MP3\)](#) • [Watch the video](#) • [Presentation](#)  • [Presentation](#) 