The Federal Reserve's Payment Security Strategy Next Steps

Ken Montgomery, First Vice President and Chief Operating Officer,
Federal Reserve Bank of Boston
Secure Payments Strategy Leader, Federal Reserve System

FedPayments Improvement Community Forum
October 3, 2018

Good afternoon. I'm happy to be here at the first FedPayments Improvement Community Forum to discuss the next steps in the Fed's secure payments strategy. In fact, today marks the beginning of the next phase in the Fed's work with the industry to advance payment security.

But first, for those of you who don't know me, I'm first vice president and COO of FRB Boston. Last December, I was named to head the Federal Reserve's secure payments strategy. As you know, the Fed has been proud to serve as a catalyst for change and a leader in working with industry stakeholders to advance U.S. payment security.

I'll highlight the work of the Secure Payments Task Force that was active from June 2015 to March 2018 and included over 200 participants. During its tenure, the task force provided advice on payment security matters. It coordinated with the Faster Payments Task Force to identify solutions for payment speed and security and helped the Faster Payments Task Force define security as part of the overall faster payments effectiveness criteria. The Secure Payments Task Force also determined priorities for future action to advance payment system safety, security and resiliency. Task force work groups looked at issues related to payment identity management, data protection and payments fraud information sharing, which helped define our priorities and the additional activities in payment security that I will discuss in a few minutes. Some deliverables of the task force included the Information Sharing Data Sources and Payment Lifecycles and Security Profiles, which have been downloaded more than 1,000 times to date. These have proven to be valuable resources to help identify issues and improve U.S. payment security.

Our future work to advance payment security rests on a strong foundation built by the Secure Payments Task Force. Many task force participants are here today. We thank them for their contributions.

While the Secure Payments Task Force has concluded, our collective work in secure payments is far from over. You likely see some of the same reports I do on cybersecurity incidents. Last Friday, Facebook announced that an attack on its network exposed the personal information of nearly 50 million users. The U.S. Treasury has issued cyber-risk warnings to large U.S. banks, which have seen an uptick in attempted cyberattacks in recent weeks. Last year, more than a million children had their identities stolen, fueling payments fraud.

The persistence and increasing scale and sophistication of the threats we face create an imperative for ongoing collaboration.

For the past several months, staff at the Fed has focused on an assessment to determine what this next phase of collaboration on payment security will look like. Based on feedback from the task force and industry, we have identified five areas of focus for consideration: endpoint security, identity authentication, data protection, fraud information sharing, and secure interconnectivity of emerging payments.

The Fed also sponsored secondary research by the Boston Consulting Group on payments fraud and security vulnerabilities to help provide an objective analysis and validate our areas of focus. Questions we asked included: What is the incidence and cost of fraud across channels? What are the fraud causes and contributing factors? Where are the data gaps? What don't we know? BCG reviewed surveys, academic literature and industry reports and conducted targeted industry interviews to inform gaps in its secondary research.

In addition, we set parameters for the Fed's next steps to address what we believe to be issues of common concern. As a leader and catalyst for change, where can the Fed help the industry accelerate its progress? Where are the gaps in payment security efforts – such as the newness or breadth of a problem, lack of coordination, or varying opinions on how to best address it? Where can we complement work already going on in the industry?

We have continued to talk with industry stakeholders about their issues and priorities for advancing payments security – and now, we want to continue the dialogue with you.

Transparency, collaboration and inclusiveness have been hallmarks of the Federal Reserve's work to improve payments. As we move forward, we'll continue with those principles. We welcome your input on the ideas we're putting forth today . . . and your continued involvement through the FedPayments Improvement Community.

In the meantime, I'll highlight three themes we have uncovered through research, input from the Secure Payments Task Force and ongoing payments industry discussions.

<u>Theme #1</u>: U.S. payments fraud has continued to grow.

The Fed's first comprehensive estimate of non-cash, non-wire payments fraud was $6.4 billion in 2012. We're awaiting updated fraud data from the Fed's payments study that will be released later this month. In the meantime, the BCG secondary research suggests that non-cash, non-wire payments fraud were close to $10 billion in 2016. Add in wire fraud, and the number is even bigger.

The overall fraud rate for all payment methods combined increased between 2012 and either 2015 or 2016, depending on the study. In looking at fraud trends by payment method, we can see how fraud moves to the path of least resistance. So, when we address individual

vulnerabilities, we need to think beyond the short-term effects to the longer-term consequences.

This research reinforces the need for us to take a collaborative and holistic approach. We need to overcome incentives and behavior that simply "squeeze the balloon" and push the problem to other channels or stakeholders.

Theme #2: Data gaps across payment methods and stakeholder groups make it more difficult to assess – and address – payments fraud. For example, there is relatively little data on ACH, wire and check fraud, or on business payment fraud. Not surprisingly, various studies define and categorize fraud types, causes and costs in different ways and over different timeframes.

Given the data gaps, our very rough estimate based on the secondary research is $7 billion to $15 billion in fraud-associated costs in 2016. In other words, the cost of mitigation and remediation may be almost equal to, or greater than, gross fraud.

Our experience with the study demonstrates the need for a more methodical approach to tracking fraud and fraud costs across the payment system. It also aligns with the task force's conclusion that we need more and better data and information sharing.

Theme #3: We are gaining insights on where fraudsters are exploiting vulnerabilities in the U.S. payment system. For example, we see uneven resources and capabilities to combat fraud. Fraudsters exploit the weakest links and highest-return opportunities in the payments ecosystem, including vulnerable endpoints, people, technology and organizations that may lack fraud-fighting resources and experience.

We also see reliance on static data that often is compromised. Payment and account verification relies on Social Security numbers, account numbers, routing and transit numbers and card expiration dates. Much of this static information is available to fraudsters due to data breaches – and sometimes, oversharing on social media. Again, this is consistent with our hypothesis going-in that endpoint security and data protection are keys to payment security improvement.

As we learn more about these and other payments fraud issues, we're also seeking ways to address them. The Fed has identified four priorities for near-term action based on research, input from the Secure Payments Task Force and ongoing payments industry discussions. We'll talk about the first three of these priorities in more detail at this Forum over the next day and a half.

Our first step in addressing the gaps in insights and information about fraud will be to collaborate on ACH and wire fraud definitions. If we don't know where fraud is occurring, it's difficult to address it – but there's wide disparity in how payments fraud losses are reported and a relative dearth of research on ACH and wire fraud. Our intended work products are to develop ACH and wire fraud definitions, as well as a roadmap to encourage broad industry

acceptance and use of these definitions in reporting. We believe the benefits to be derived by this include an enhanced understanding of fraud scope and risk; reduced misclassification of fraud and improved mitigation, including through third-party services; and easier collaboration for national and international fraud mitigation.

The approach we want to take is to form a Fed-led work group in collaboration with the payments industry, starting later this year, with a nine- to 12-month horizon for delivery. The work group will be composed of 20 to 30 industry and Fed participants with specific relevant expertise, such as fraud systems technology, and representing diverse industry segments.

Two additional areas of focus will follow this first work stream.

Synthetic identity payments fraud is a combination of real information, such as a Social Security number, and fictitious information to create a fake identity used to defraud or evade payments safeguards. This type of fraud is rising due to large-scale data breaches, use of static information for identification, the shift to remote payments channels and remote applications for payment accounts, a lack of identifiable victims reporting fraud – and high payoffs for fraudsters.

The desired outcome of this work stream is a better understanding of synthetic identity payments fraud that improves our ability to address it. Outcomes could include more consistent definitions, reduced miscategorization of synthetic identity payments fraud as chargeoffs, and improved understanding of trends and red flags. We also would like to foster collaboration between the industry and federal agencies to identify and advance approaches to mitigate and reduce fraud.

Over the next several months, we seek a dialogue with the industry on this type of fraud. What actions could the Fed take? Where are the priorities? The Fed's actions over the next year or so could include research, education, advocacy, thought leadership and collaborative work efforts, whether Fed-led or the Fed's participation in existing work groups.

Our third area of focus is remote payments fraud mitigation. What we see as the industry need is to address increasing remote payments fraud that encompasses payments across ACH, wire, debit and credit cards. Online businesses face a bigger challenge authenticating and securing remote payments. Authentication methods vary across stakeholders, channels and payment methods – and some are more effective than others.

What we see as the desired outcome and benefit of this effort would be broad industry alignment on effective authentication approaches and methods that would help mitigate remote payments fraud and strengthen endpoint security.

Over the next several months, we likewise seek a dialogue with the industry on potential actions and priorities. Fed actions could include research, education, thought leadership and collaboration. This topic also came up at the Chicago Payments Symposium earlier today. There

are remote payments authentication solutions available – what can we do collectively to advance their widespread use? Where are the gaps?

In addition to these three work streams that will be discussed here at the Forum, the Federal Reserve is looking for ways to facilitate information sharing and strategic dialogue on evolving payment security and fraud issues – which ties into the Fed's faster payments work, as well. Federal Reserve staff members continue to participate in industry work groups and information sharing forums, such as the NACHA Payments Alliance, X9 and FS-ISAC.

I mentioned earlier that we are focused on addressing areas of common concern and undertaking these efforts in our leader and catalyst role in the payment system. The output of these work streams could include white papers on the scope of the issues, observations on potential mitigation steps and other related recommendations on next steps. We don't see the output as policy or regulations. Likewise, we are mindful that work by other entities is under way in several of these areas. It is not our intent to duplicate or redirect any ongoing efforts, but to collaborate as appropriate.

We want your input. Over the next day and a half, we'll hold four workshops to seek your input on advancing the work streams I discussed. This includes two sessions on ACH and wire definitions fraud, one immediately after the break today and one tomorrow. We want to make sure everyone has the chance to attend one of these sessions, since this will be our first initiative later this year or early next year. We also will hold one session on remote payments fraud immediately after the break today. Another workshop on synthetic identity payments fraud will occur tomorrow morning.

Our questions for you include: As a leader and catalyst, where can the Fed help the industry accelerate its progress? We've identified four priorities for near-term action. Should we consider other priorities in lieu of these, or once these work efforts wind down?

We value your partnership. The U.S. payment system continues to evolve to meet the needs of an economy that's increasingly global, digitally interconnected, real-time and information-driven. Industry collaboration is the foundation of this successful evolution. Together, we can help create a faster, more secure and efficient U.S. payments infrastructure.

We thank you for your continued involvement and support. The Secure Payments Task Force laid a foundation for continued progress in payment security. While our future work will be more targeted, it can only be successful with your involvement and support. Thank you in advance for your contributions.