

**An Update on the Federal Reserve's Efforts to
Modernize the Payment System**



**Loretta J. Mester
President and Chief Executive Officer
Federal Reserve Bank of Cleveland**

**Keynote Speech
2022 Chicago Payments Symposium:
Building Customer-Centered and Adaptive Networks
Federal Reserve Bank of Chicago
Chicago, IL**

October 4, 2022

Introduction

I thank Ellen Bromagen and the other organizers for inviting me to speak again at the Chicago Payments Symposium. It is truly an honor to participate in this symposium, which, under Ellen's leadership, is a premier event for sharing ideas and for gathering insights from those who are involved in the payment system. At this time of dramatic change in payments, I feel privileged to chair the Fed's Financial Services Policy Committee (FSPC), which oversees the provision of the Fed's payment services to deposit institutions and the U.S. Treasury. And I want to thank Ellen for being such a key member of our committee, providing insights from her years of experience working in payments. I would also like to take this opportunity to extend my sincere appreciation to Federal Reserve Bank presidents Charles Evans and Esther George, who will be stepping down from their roles in January. Throughout their careers at the Fed, Charlie and Esther have been strong and dedicated leaders working on behalf of the public. They have made important contributions to all aspects of the Fed's work, including monetary policy, banking supervision, financial stability, community development, and payments. Indeed, their leadership has been instrumental in the System's success in supporting the ongoing modernization of the payment system. I am very grateful to count Esther and Charlie as friends and I appreciate their mentorship – although they may have wished for a better student.

This morning, I will discuss some efforts the Federal Reserve has underway, in collaboration with the industry and other payments stakeholders, to modernize the payment system, a critical part of the infrastructure in the U.S. Of course, the views I present will be my own and not necessarily those of the Federal Reserve System or of my colleagues on the Federal Open Market Committee (FOMC).

The Fed's Modernization Efforts

Because the current payment system works well, most people have spent little time thinking about the backbone that makes these payments possible and ensures that the payment system is reliable and secure. This rational inattention is just as it should be. But with the changes brought by new technology and the

entry of new service providers, more people are seeking new ways to execute transactions, whether it be online or via cell phone, and they want to execute them faster. The modernization efforts underway aim to foster a system that is not only efficient, secure, and effective, but also one that is innovative, adaptable, resilient, and accessible to everyone: a payment system that consumers and businesses can rely on with confidence to efficiently make purchases, pay bills, and get paid. Indeed, ensuring that the public can be confident in the system is a critical ingredient in achieving a better payment system, so innovations aimed at efficiency must also be designed for security and resiliency.

The Federal Reserve has taken a collaborative approach in its modernization efforts. Ten years ago, the Fed recognized that the payment system was at an inflection point. New technologies were being developed and increasingly used, and the expectations of the end users of the payment system were also evolving. These conditions portended a period of rapid transformation in the end-to-end payments landscape. The Fed engaged with a diverse set of payment-system stakeholders, and we all came to agree that the U.S. payment system needed to evolve further and faster to support the changing nature of commerce, keep pace with the global economy, meet the changing needs of end users and offer them better value, and address new and ongoing threats to security. Again engaging with stakeholders, the Fed established strategies to improve the payment system in terms of the speed, security, and efficiency of domestic and cross-border payments.¹ These strategies, along with tactics, were published in 2015 and they have guided the Fed's modernization efforts.

Over the ten years since the Fed recognized that the U.S. payment system needed improvement, two things have happened. First, as foreseen, the payments landscape has undergone significant change. New entrants, shifting user needs, and digitalization have all shaped new models and methods for making payments. Traditional providers and fintech firms are coming to market with products that better meet

¹ See Federal Reserve System (2015).

customers' needs in terms of convenience and that address long-standing frictions in the payment system. New technologies have shaped the public's expectations for faster, more efficient, and broadly accessible payment services that, at the same time, are safe and secure.

The second thing that has occurred is considerable progress toward the goal of a better payment system that benefits all, a goal shared by the Federal Reserve, the industry, and end users. What both the private sector and the public sector have accomplished in a relatively short period of time is impressive, particularly given the complexity and interconnectedness of the U.S. financial infrastructure. This progress underscores the value of collaboration. Indeed, the Fed working collaboratively with a broad array of payment participants was one of the five strategies included in our 2015 paper that catalyzed our current modernization efforts.

Let me now touch on a few examples of current and future innovations.

Current Payment Innovations

Digital payments

Innovative digital payments products are filling gaps, addressing inefficiencies, and expanding payments access to underserved consumers. According to a 2021 Fed survey, nearly seven out of 10 consumers use mobile payment devices to send or receive payments, and this usage spans consumers of all ages.² This is a considerable increase from 2013, when only one in 10 consumers had ever made a mobile payment. In addition to using services from their primary bank or credit union, 83 percent of consumers are using a digital wallet or a fintech payment app at least occasionally to complete transactions, including 71 percent of those age 55 and older.³

² See FedPayments Improvement (2022).

³ See FedPayments Improvement (2022).

Of course, the pandemic has had a wide-ranging and uneven impact on firms' and households' payment behaviors and patterns. The share of retail sales done electronically jumped during the pandemic, but this share began increasing much earlier. According to the U.S. Census Bureau, e-commerce sales accounted for about 6 percent of total U.S. retail sales in 2013. That share has now risen to about 14 percent.⁴ It seems clear that the consumer's preference for digital payments, which has been spurred by industry innovation, is here to stay. Apps created by financial institutions and fintech providers are increasingly easy to use and access. Other digital tools have significantly improved money management and financial access for consumers, including those with low or moderate incomes, who have historically been underserved. At the same time, because maintaining the public's confidence in the payment system is a public good, it is important to ensure that consumers using these new payments products understand how these new products compare with other payment instruments, including cash, in terms of risks and benefits. Ensuring that new products and payments rails are built with security and resiliency in mind from the very start is essential if the modernization of the payment system is to live up to its promise.

Combating fraud and increasing cyber resilience

One negative trend affecting the payment system is the increase in fraud. Fraud has the potential to undermine the public's confidence in the payment system, and staying ahead of the fraudsters requires constant vigilance because of the increasing sophistication of the frauds being perpetrated. Scams abound and are constantly changing. Bad actors are hacking into systems by using bots, phishing schemes, and social networks to exploit weaknesses in the system. Payment fraud comes in a variety of forms. According to one estimate, synthetic identity fraud, in which personal identifiable information such as a Social Security number is used to fabricate a person or entity in order to commit a fraudulent act,

⁴ See U.S. Census Bureau (2022). In this report, e-commerce sales are "sales of goods and services where the buyer places an order, or the price and terms of the sale are negotiated over an Internet, mobile device (M-commerce), extranet, Electronic Data Interchange (EDI) network, electronic mail, or other comparable online system. Payment may or may not be made online."

accounted for \$20 billion in losses for U.S. financial institutions in 2020.^{5, 6} Remote authentication fraud, in which a new account is fraudulently created in someone' else's name, or a victim's account is taken over by using stolen credentials or information, is also on the rise.⁷

To help its financial institution customers better fight fraud, the Fed has published a series of research briefs and has expanded educational resources in concert with industry participants. The FraudClassifierSM model is a good example of our recent efforts with the industry. The model can be used regardless of the payment type, payment channel, or payment characteristics to facilitate more consistent fraud classifications. This can help an organization improve its fraud management and responses, as well as more effectively educate its customers on current fraud methods and how to protect themselves.⁸

The Fed is also working constantly to strengthen the defenses and enhance the resilience of our clearing and settlement platforms. While we have remained secure from ever-growing cybersecurity threats, we do not take that for granted. We are continuously working to enhance the cybersecurity and resiliency of our own systems, applications, and data, to ensure that we can detect and prevent an attack on our systems, and if one were to occur, making sure we can minimize the time it takes to contain it and limit the business impact on our customers and the broader public. We regularly obtain cyber intelligence on how actors may attempt to attack critical Federal Reserve payment systems; we regularly test our controls to determine their capabilities in preventing these attacks from being successful; and we are continuously improving and testing our preparedness against a potential ransomware attack, which is a top threat for organizations, including the Fed.

⁵ See FedPayments Improvement (2019).

⁶ This estimate comes from software company FiVerity. See ABA Banking Journal (2021).

⁷ See FedPayments Improvement, "Remote Authentication Fraud."

⁸ See FedPayments Improvement, "FraudClassifier Model."

e-Invoicing

The Fed is also focused on enhancing payment efficiency. Just like consumers, American businesses are eager to go electronic with payment options that provide immediate access to funds and support straight-through processing of invoice, payment, and remittance data. Despite that desire, check usage remains high for business-to-business (B2B) payments because current electronic options pose challenges for payments reconciliation. To help remedy this impediment, the Fed is collaborating with the Business Payments Coalition to modernize B2B payments. One of the fruits of that collaboration is the e-invoice exchange market pilot. This is an effort to build and test a virtual network that will enable businesses of all kinds to exchange e-invoices by establishing a secure and open delivery framework between providers.⁹ The collaboration has also determined that the electronic exchange framework could be adapted so that businesses could share with one another a payment's remittance information.

Faster payments infrastructure

Perhaps the most visible and eagerly anticipated innovation in payments is the establishment of instant payment capabilities. In the Fed's 2021 payments survey, 62 percent of consumers said they expected to be using faster payment options more extensively in the future, particularly options that offer robust fraud protections.¹⁰ Meanwhile, nearly two-thirds of businesses we surveyed in 2020 said that they would factor access to faster payments into future decisions on whether to switch banks.¹¹

The industry has made great strides in offering faster payments, and building in security features, including identity management, authentication, and robustness. Real-time settlement is an important security feature of faster payments. When settlement is deferred, the payee's service provider is taking on credit risk until it gets the funds from the payer's service provider. To reduce this risk, some, but not all,

⁹ See Business Payments Coalition, "Electronic Invoices."

¹⁰ See FedPayments Improvement (2022).

¹¹ See FedPayments Improvement (2021).

of the faster payment systems around the world couple real-time or near real-time settlement with faster payments.¹²

The Federal Reserve will launch its own instant payments rail incorporating real-time clearing and settlement, the FedNowSM Service, between May and July of next year.¹³ As was discussed yesterday at the symposium, the Fed's goals in offering instant payments through FedNow include providing greater flexibility to consumers and businesses through instant access to their funds; increasing access to the payment system for more consumers; offering the potential for greater efficiency in B2B payments by including invoice and remittance data within payment messages; and leveling the playing field for competition. This faster-payments rail and the innovation that will emerge around it hold great promise in making both domestic and cross-border payments more efficient and more accessible to all.

The Fed has spent several years planning for and investing in FedNow and its launch is fast approaching. Financial institutions will be able to connect to the service either directly, via their core processors, or through a technology service provider. Now is the time for industry stakeholders, including financial institutions and core service providers, to prepare themselves to use the new service, and the Fed is leaning in on stakeholder engagement to ensure everyone is ready. Our pilot testing program has more than 120 participants and our FedNow Community portal is a great place to get information.¹⁴ We realize that for many financial institutions, getting ready to use FedNow will take some investment. Some organizations will need to upgrade 40-year-old payment infrastructures, accounting procedures, and other back-office processes to accommodate the expanded 24×7 operating hours. But the Fed is asking you to

¹² See Mester (2017) and Committee on Payments and Markets, Bank for International Settlements (2016).

¹³ See Brainard (2022) for an update on FedNowSM.

¹⁴ Information on joining the FedNow Community is available at <https://www.frb.services.org/financial-services/fednow/community>.

make those investments so that you'll be prepared to offer this new instant payments service to your customers, who are increasingly demanding faster payments.

Future Payment Innovations

As we continue to make improvements to the payment system today, we also have to prepare for the future. It is important for us to ensure that our payment system evolves in a productive way. Innovation, competition, collaboration, broad accessibility, common standards, risk management, and appropriate supervision and regulation – all are important facets of a well-functioning payment system.

Diversity of providers and technologies

Innovation in payments is not going to stop. Partnerships between traditional financial institutions and newer fintech firms are becoming more common. Indeed, many fintech firms have participated in the Federal Reserve's FedNow Service Provider Showcase, a one-stop resource that connects financial institutions and businesses with service providers who can help them implement instant payment products using the FedNow Service. Financial institutions are exploring opportunities to improve both back-office and customer-facing operations in partnership with fintech firms.^{15, 16} Many banks now use application programming interfaces (APIs) and other tools to provide the underlying financial infrastructure to nonbank technology firms and their customers, including deposit services and access to the payment rails. Fintechs are increasingly becoming significant providers of technological services to smaller banks, which lack the scale to develop such technologies on their own.

The growing diversity of the providers of payment services, including nonbank and fintech firms, is likely to continue. New tools and techniques previously unavailable to some financial institutions, including

¹⁵ See Bowman (2022).

¹⁶ See Board of Governors of the Federal Reserve System (2021).

machine learning and artificial intelligence, are now being applied to credit underwriting, back-office operations, and various aspects of risk management. And learning how to apply these new technologies more effectively is ongoing. For example, it is now better recognized that just because it is an algorithm does not mean it is immune from producing discriminatory underwriting and pricing decisions. Testing algorithms before they are deployed and designing so-called ethical algorithms, which balance the accuracy of a credit-risk model with other goals such as not producing systematically higher error rates for one racial group than another, are methods that can be used to avoid unintended consequences of the new tools.¹⁷

Just like the industry, the Fed is actively monitoring and studying new technologies and approaches to payments, and we are enhancing some of our service offerings to help our customers offer better services to theirs. For example, last month Fed Financial Services launched the FedPayments® Insights Service, an analytical tool that generates reports on a financial institution's payments settled through the FedACH® Service to help inform business strategy and day-to-day ACH operations.¹⁸ We continue to provide APIs to improve payment system efficiency and accessibility.¹⁹ And so that we will be better positioned to meet our customers' needs and those of the public, we have changed how Federal Reserve Financial Services are organized within the Fed. As many of you know, for the past 20 years, we have organized financial services by product line, such as wholesale, retail, and cash. This year we have restructured our services along functional lines, such as technology, operations, and customer service. Mark Gould, who spoke yesterday, serves as our chief payments executive, overseeing Fed financial services.

¹⁷ See Mester (2020b) and Kearns and Roth (2020) for further discussion.

¹⁸ See FRBServices (2022).

¹⁹ Examples include our Service Status API, which monitors the availability of Fed financial services in real-time; FedCash Services E-Manifest API, now active as a pilot program, which gives financial institutions and armored carriers greater ability to track currency shipments from order to delivery; and FedNow Service APIs, which will launch next year and report transaction details, update status and daily activity, and provide downloadable information to customers. See FRBServices.org for more information.

Central bank digital currency

The Fed, under direction from the Board of Governors, is also exploring emerging technologies and evaluating whether there is a potential role for a U.S. central bank digital currency (CBDC) in the future.

The Federal Reserve has been researching issues raised by a CBDC for some time. To foster public dialog, earlier this year the Board of Governors released a discussion paper outlining potential benefits, risks, and policy considerations of a U.S. CBDC and invited public comment.²⁰ As readers of that paper know, there are numerous issues pertaining to CBDC that have to be evaluated including the implications for financial stability, global financial market functioning, and the transition of monetary policy; how to ensure security and balance privacy with transparency; and whether there is a use case for CBDC in the U.S. No decision has been made about whether to issue a U.S. central bank digital currency.

Nonetheless, given the evolving digitalization of the financial system, under coordination by the Board of Governors, the Federal Reserve System is researching and experimenting with the underlying technologies.²¹ We are gaining insights that will not only help inform a future decision on a CBDC but also aid our current work on faster payments, interoperability between payment systems, and payment system resiliency.

Payment security and consumer safeguards

As the payment system evolves, the safeguards needed to maintain the public's confidence in the payment system will also need to evolve. Private-sector and public-sector service providers and regulators need to ensure that user protections are in place for responsible data use and privacy, and that safeguards adequately protect customer accounts against cybersecurity breaches, fraud, and data leakage. It is also our collective responsibility to educate consumer and business users of the payment services so they can take appropriate steps to protect themselves from fraud and understand the risks, which may vary across

²⁰ See Board of Governors of the Federal Reserve System (2022a).

²¹ Mester (2020a) and Mester (2020b) discuss some of the experimentation taking place.

products and services, especially while there is variation in the consumer protections in place. And it is incumbent upon providers and regulators to continue to educate themselves as new technologies emerge. For example, once quantum computing fully develops, it will disrupt the cryptography currently in place that secures our payment services. Data privacy methods will also have to adapt. The traditional way of keeping data private, by taking away names or otherwise anonymizing it, no longer works in a world rich with multiple data sources that can be cross-referenced to de-anonymize the data and reveal identities.²² So we can't take for granted that our current methods for securing our payment system will remain valid; as technologies evolve, we need to evolve our methods as well.

Payment system supervision

How we go about effectively supervising the payment system will also need to evolve to ensure that the system remains secure, effective, and broadly accessible. The public policy approach will need to change to include a more holistic blending of financial regulation, antitrust policy, and data privacy regulation. To ensure that the benefits of a better payment system are captured and the risks managed, there will need to be cooperation across these types of regulators, as well as international cooperation through the Financial Stability Board and other international entities, given the global nature of payments and the entities that are now offering payments services. Extending some regulations to new services is already occurring; for example, payments services offered by bigtech firms are subject to "know your customer" rules.

As new providers enter the field, we'll need to focus more on the risks a service entails rather than on the type of entity providing the service. This will help limit regulatory arbitrage while at the same time supporting financial stability and innovation. This risk-focused approach is seen in the final guidelines

²² See Mester (2020b) for further discussion. Kearns and Roth (2020) discuss how then-Massachusetts governor William Weld's medical record was identified by combining the anonymized medical records released by the state with voter registration data.

approved by the Board of Governors in August that Federal Reserve Banks will use when evaluating requests from institutions for access to Fed accounts and payment services.²³ The guidelines incorporate a three-tiered review framework that entails more extensive review for entities that entail greater risks. They aim to increase transparency and to foster equitable national treatment of account requests while supporting responsible innovation and appropriate risk management.

Conclusion

A well-functioning and secure payment system is vital to our economy. As we modernize the payment system, it is important to remember that the foundation of a successful payment system is the public's confidence in it: confidence that it will be available whenever the customer needs it; confidence that it will efficiently route and settle payments; confidence that it will be resilient against cyber attacks and fraudulent actors; and confidence that it can be relied upon without having to know the intricacies of the infrastructure behind it. This confidence requires trust in the financial entities offering payment services. Today, the American public does have confidence in the payment services offered by the Federal Reserve System and the industry. But we cannot take that for granted. As the payment system evolves, the Fed, the industry, and end users will need to continue to collaborate to ensure that the modern payment system lives up to its promise of being efficient, safe, resilient, and available to all. That's the best way to maintain the confidence of the public we serve.

²³ See Board of Governors of the Federal Reserve System (2022b).

References

- ABA Banking Journal, “Report: Synthetic Identity Fraud Results in \$20 Billion in Losses in 2020,” October 20, 2021.
(<https://bankingjournal.aba.com/2021/10/report-synthetic-identity-fraud-results-in-20-billion-in-losses-in-2020/>)
- Board of Governors of the Federal Reserve System, “Community Bank Access to Innovation through Partnerships,” September 2021.
(<https://www.federalreserve.gov/publications/files/community-bank-access-to-innovation-through-partnerships-202109.pdf>)
- Board of Governors of the Federal Reserve System, “Money and Payments: The U.S. Dollar in the Age of Digital Transformation,” January 2022a.
(<https://www.federalreserve.gov/publications/money-and-payments-discussion-paper.htm>)
- Board of Governors of the Federal Reserve System, “Federal Reserve Board Announces Final Guidelines That Establish a Transparent, Risk-Based, and Consistent Set of Factors for Reserve Banks to Use in Reviewing Requests to Access Federal Reserve Accounts and Payment Services,” August 15, 2022b.
(<https://www.federalreserve.gov/newsevents/pressreleases/other20220815a.htm>)
- Bowman, Michelle W., “Technology, Innovation, and Financial Services,” VenCent Fintech Conference, Little Rock, Arkansas, August 17, 2022.
(<https://www.federalreserve.gov/newsevents/speech/bowman20220817a.htm>)
- Brainard, Lael, “Progress on Fast Payments for All: An Update on FedNow,” at FedNow Early Adopter Workshop, Rosemont, IL (via webcast), August 29, 2022.
(<https://www.federalreserve.gov/newsevents/speech/brainard20220829a.htm>)
- Business Payments Coalition, “Electronic Invoices.”
(<https://businesspaymentscoalition.org/electronic-invoices/>)
- Committee on Payments and Market Infrastructures, Bank for International Settlements (2016), “Fast Payments – Enhancing the Speed and Availability of Retail Payments,” November 2016.
(<http://www.bis.org/cpmi/publ/d154.pdf>)
- FedPayments Improvement, “FraudClassifier Model.”
(<https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/>)
- FedPayments Improvement, “Synthetic Identify Fraud in the U.S. Payment System: A Review of Causes and Contributing Factors,” *Federal Reserve Payments Fraud Insights*, July 2019.
(<https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf>)
- FedPayments Improvement, “Businesses Look to the Future with Faster Payments,” *Federal Reserve Market Readiness Brief*, August 31, 2021.
(<https://fedpaymentsimprovement.org/wp-content/uploads/pandemic-spurs-faster-payments-demand.pdf>)
- FedPayments Improvement, “Today’s On-Demand Lifestyle Is Spurring Greater Demand for Faster Payments,” *Federal Reserve Market Readiness Brief*, May 16, 2022.
(<https://fedpaymentsimprovement.org/wp-content/uploads/federal-reserve-consumer-research.pdf>)

FedPayments Improvement, “Remote Authentication Fraud.”

(<https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/remote-authentication-fraud/>)

FRBServices, FedPayments® Insights Service press release, September 19, 2022.

(<https://www.frbervices.org/news/press-releases/091922-fedpayments-insights>)

Federal Reserve System, “Strategies for Improving the U.S. Payment System,” January 26, 2015.

(<https://fedpaymentsimprovement.org/wp-content/uploads/strategies-improving-us-payment-system.pdf>)

Kearns, Michael, and Aaron Roth, “Ethical Algorithm Design Should Guide Technology Regulation,” report from the Brookings Institution’s Artificial Intelligence and Emerging Technology Initiative, January 13, 2020.

(<https://www.brookings.edu/research/ethical-algorithm-design-should-guide-technology-regulation/>)

Mester, Loretta J., “Updates on the Economy and the Federal Reserve’s Payments System Improvement Initiative,” Tenth Annual Risk Conference: Promise and Peril: Managing the Uncertainty of Rapid Innovation and a Changing Economy, Federal Reserve Bank of Chicago and De Paul University Center for Financial Services, March 30, 2017.

(<https://www.clevelandfed.org/en/newsroom-and-events/speeches/sp-20170330-updates-on-the-economy.aspx>)

Mester, Loretta J., “Payments and the Pandemic,” Keynote Session, 20th Anniversary Chicago Payments Symposium, Federal Reserve Bank of Chicago (via videoconference), September 23, 2020a.

(<https://www.clevelandfed.org/newsroom-and-events/speeches/sp-20200923-payments-and-the-pandemic>)

Mester, Loretta J., “Fintech, Bigtech, and Financial Inclusion,” Fourth Annual Fintech Conference, Federal Reserve Bank of Philadelphia (via videoconference), November 9, 2020b.

(<https://www.clevelandfed.org/newsroom-and-events/speeches/sp-20201109-fintech-bigtech-and-financial-inclusion>)

U.S. Census Bureau, “Quarterly Retail E-Commerce Sales: 2nd Quarter 2022,” August 19, 2022.

(https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf)