Remarks by Assistant Secretary for Financial Institutions Graham Steele on the Digitization of Financial Services at the Transform Payments USA 2023 Conference

June 13, 2023

AUSTIN, TX - Today, Assistant Secretary for Financial Institutions Graham Steele delivered remarks at the Transform Payments USA conference in Austin, Texas on the digitization of financial services.

As Prepared for Delivery

Good morning,

Thank you for having me. I am Graham Steele, Assistant Secretary for Financial Institutions at the Treasury Department, and it is a privilege to be here with you today.

As the Assistant Secretary for Financial Institutions, I am responsible for the Treasury’s policy views on matters affecting banks, credit unions, insurance, consumer protection, access to capital, and financial sector cybersecurity.

The discussions at Transform Payments USA reflect the larger, decades-long trend of the digitization of financial services. Over the past 30 years, we went from less than 1% of the world’s population having access to the internet in the 1990s to over 60% of world being internet users today.[1] This digital expansion has brought about an era of incredible opportunities and novel risks in financial services, sparked by advancements in computing power and connectivity. We have found ourselves in an age of rapid change and development, and there are a number of significant developments that I will highlight today. These include the forthcoming launch of FedNow, continued exploration of Central Bank Digital Currencies (CBDCs), and the evolution of Open Banking. All of these efforts have the potential for profound, far-reaching impacts on consumer privacy, financial inclusion, fraud prevention, and the changing roles of firms within the financial system. The offices I oversee at Treasury are at the vanguard of these cross-cutting policy issues.

FedNow
I’ll begin with FedNow, the Federal Reserve’s highly anticipated service for faster payments. This 24x7x365 service will provide U.S. depository institutions, as well as U.S. branches of foreign banks, with the ability to send and receive interbank payments instantly. It marks a pivotal shift in our public payments infrastructure, fundamentally altering the payment settlement structure by facilitating direct, real-time gross settlements (RTGS) for interbank payments. This means that transactions can be settled nearly instantly, foregoing deferred net settlement. Further, the introduction of FedNow adds another crucial element to the payments landscape by creating a second operator alongside the existing private sector Real-Time Payments (RTP) network operated by The Clearing House. Having multiple payment operators promotes choice and competition in payments, driving innovation and encouraging the development of new payment services and features. It can also enhance resiliency in the payments system by providing redundancy that helps ensure that disruptions or outages in one operator do not completely halt the flow of transactions.

In thinking about the rollout of FedNow and its potential impacts, it is worth examining international developments to consider what we can learn from the experiences of other countries. The United Kingdom’s Faster Payments Service (FPS) is one example of the feasibility and benefits of faster payment systems. Launched in 2008, this service operates around the clock, enabling secure and near real-time transfers of funds between accounts at different institutions. In 2022 alone, the Faster Payments Service processed over 3.9 billion payments with a total value exceeding £3.2 trillion, showcasing its scale and robustness. The success of the UK's FPS signaled the transformative potential of faster payment systems in improving transaction capabilities with speed, efficiency, and inclusivity. As highlighted in Treasury’s recent report on the Future of Money and Payments, international experience suggests that broadening the range of institutions that are eligible to participate in instant payment systems—for certain limited purposes and subject to appropriate guardrails—could help to enhance speed and efficiency, competition, and inclusion in payments, including for cross-border payments.

At the same time, we must keep in mind that faster payments also require responsive risk-management, error identification, and fraud response. With the ability to move money instantaneously between accounts, we face potential fraud scenarios that are more complex and intricate than in traditional deferred settlement payment systems. To mitigate this, we need to consider how we can harness technology and policy to help mitigate risks. Some have suggested an approach that could include tools like advanced cryptographic methods, multi-factor authentication, programmatic anomaly detection, as well as prudent operating and governance procedures with safeguards like transactional limits. A thoughtful and comprehensive approach
will be crucial in maintaining trust in the payments system, and ultimately, helping to ensure its success.

It is worth noting that FedNow has adopted ISO 20022 (ISO twenty ou two two), the global messaging standard for modern payments. ISO 20022's remittance data standard accommodates transmission of an extended amount of data, allowing for richer information to accompany each transaction. This feature could be instrumental in tracking funds and identifying fraudulent activity more efficiently.

Treasury will continue to work with the broader sector to ensure that we are keeping the instant payments system safe and resilient for the American consumer. In December, for example, Treasury’s Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) published an advisory to warn of holiday scams and alert consumers to emerging trends in the fraud landscape.

Treasury sees the value in encouraging the use of instant payments to support a more competitive, efficient, and inclusive U.S. payment landscape. To that end, Treasury has signed up as an early adopter of the FedNow payment service. While the vast majority of government payments are regular, predictable, and scheduled, we are piloting the usage of FedNow for payments where speed is particularly important.

**CBDC, PRIVACY, AND FINANCIAL INCLUSION**

Many jurisdictions around the globe are also exploring Central Bank Digital Currencies (CBDCs) as an option for upgrading money and payments infrastructure. To be clear, the United States has not yet determined whether it will pursue a CBDC. To complement the ongoing work being undertaken by the Federal Reserve, Treasury is leading an interagency working group to provide a broader Administration perspective for considering the implications of any potential U.S. CBDC. The working group is evaluating policy objectives related to global financial leadership, national security, and privacy, illicit finance and financial inclusion. Striking the right balance between these priorities, and realizing potential benefits while minimizing risks, would depend on the design of both policy and technology.

A retail CBDC, unlike central bank reserves, would be a liability of the central bank that is accessible by the general public. A retail CBDC could contribute to a more competitive and innovative payment system; support financial inclusion; and help preserve the face value redemption of the currency. The extent to which a retail CBDC would promote these objectives depends on many future design decisions, including decisions about the range of intermediaries
that would act as service providers in the CBDC ecosystem and the requirements to which those intermediaries would be subject.

Along with potential benefits, such as promoting a more competitive payment environment and financial inclusion, retail CBDCs could also pose risks, including runs into a retail CBDC that could destabilize private sector lending. As we have seen in the recent episodes of banking turmoil, a combination of technology, highly concentrated depositor base, and access to non-deposit alternatives outside of the banking system may have changed the nature and speed of bank runs. With the technology enabling the movement of deposits only getting faster, there could be additional risks associated with introduction of CBDC.

An additional challenge is protecting user privacy while minimizing risks of illicit financial transactions. Fulfilling both of these important objectives requires a careful balance in the design of any potential retail CBDC. Privacy concerns and lack of institutional trust are already among the most cited reasons that some individuals avoid the banking system. In particular, as Treasury has previously noted, some communities may be more privacy sensitive and have heightened concerns about private or public entities accessing their personal information. In this vein, it is important that we consider the extent to which privacy and anonymity might be preserved and explore the technologies and methods available, including Privacy Enhancing Technologies (PETs), to enable such protections in the design of any potential retail CBDC. Such technologies could play a crucial role in maintaining transactional privacy while also ensuring transparency and traceability, thus reinforcing the trust of users in digital financial transactions.

Another important element in the design of any potential CBDC is the degree to which it possesses offline capabilities, which could enhance resiliency and financial inclusion by allowing transactions in areas with limited or no internet connectivity. We know that a significant number of individuals in the United States lack access to reliable internet, and individuals who face barriers to mainstream financial services are also more likely to lack access to certain technology services and infrastructure. It is important to consider the needs of these marginalized communities in the design of any potential CBDC.

The CBDC working group is identifying trade-offs and possible ways of reconciling these objectives, including looking ahead to options that could reduce the size of any trade-offs.

**OPEN BANKING**

Finally, let me share some thoughts on the role of consumer data sharing in our evolving financial system. Last year, Treasury published a report assessing the impacts of new entrant non-bank
firms on competition in consumer finance markets, in response to the President’s Executive Order on Promoting Competition in the American Economy. We found, unsurprisingly, that the banking industry has grown more concentrated over time. We also noted that there are opportunities for all market participants to improve the accessibility and delivery of financial products and services.

Here, again, we can look to other jurisdictions for examples of how this might play out. In Europe, regulatory frameworks such as Revised Directive on Payment Services (PSD2) have been at the forefront of policy development, setting standards to enable secure, consumer-permissioned data sharing, which can expand access and promote competition.

In the United States, as we develop our regulatory policies, we should seek a balanced approach. Consistent with the other evolving areas that I have already discussed, we should strive to maximize the benefits and minimize the risks in any consumer data sharing framework. In the case of Open Banking, that means fostering innovation and competition while ensuring data security and consumer protection.

The rise of fintech firms and their reliance on consumer data has raised valid concerns over privacy and security risks. Practices like credential-based screen-scraping, where data aggregators store consumers' login credentials to gain unlimited access to financial data, raise concerns over privacy and liability. Fortunately, the industry has been transitioning away from screen-scraping, with initiatives to enable more secure data sharing methods, including tokenized API access. For traditional depository institutions, building APIs to facilitate secure data sharing can lead to productive collaboration with fintechs. But progress has been slow due to policy uncertainties and competitive tensions among stakeholders in the consumer finance ecosystem.

Regulatory actions recommended in the competition report – including the recent finalization of the banking regulators’ third-party risk management guidance and continued progress on the CFPB’s Section 1033 rulemaking – can provide additional clarity and security in the data sharing landscape. Recently, the CFPB convened a Small Business Review Panel to examine the impact of the Bureau’s proposals regarding consumers’ personal financial data rights. While the CFPB is still in the rulemaking process, this is a positive step towards defining the rules and responsibilities for data providers, and Treasury commends the CFPB on its comprehensive and thoughtful process for this rulemaking. Finally, I would note that Treasury’s report also recommends that the CFPB review its authorities to consider if and how the agency might supervise data aggregators.

For responsible development of the consumer data sharing ecosystem in the United States, our focus should be on protecting consumers and promoting healthy competition and innovation that enhances consumer financial well-being. As we move forward, these principles should remain our
focus in order to ensure that we are maintaining a fair and competitive financial services ecosystem.

**CONCLUSION**

As I initially noted, the focus of our dialogue during this gathering is the significant shift towards the digitization of financial services. This shift promises significant benefits but presents us with some substantial challenges. By striking the right balance as industry leaders and policymakers, we can ensure that this transformative moment in payments addresses, rather than reinforces, the shortcomings that so many experience under the current status quo. That is why I am excited to be part of this event, and I am eager to listen in on an engaging panel discussion.

Thank you for your time today.

###

[1] Individuals using the Internet (% of population) | Data (worldbank.org)

[2] Faster Payment System statistics (wearepay.uk)


