FEDERAL RESERVE BANK OF BOSTON™

Payment Strategies

REPORT

What's New with Regulation in the Mobile Payment and Fintech Space?

MPIW January 2017 Meeting with Regulators Report
May 25, 2017

By Susan Pandy, Ph.D. and Marianne Crowe, Payment Strategies, Federal Reserve Bank of Boston

Periodically, the Mobile Payments Industry Workgroup (MPIW) meets with representatives from federal and state regulatory agencies[1] to gauge their level of activity in the mobile/digital payments space and share perspectives on developments, challenges, and potential gaps in coverage or education.[2] Topics discussed at the most recent January 2017 MPIW meeting included: the role of financial technology (fintech) companies in U.S. financial services; regulatory framework for mobile/digital wallets; and an overview of the European Union's (EU) Payment Services Directive 2 (PSD2) and implications for U.S. payment industry stakeholders.

I. Fintech Innovation in the U.S.

The exponential increase in technological innovation, including the rapid proliferation of smartphones, artificial intelligence, and big data analytics, has drastically impacted the way the financial services industry operates. The term "fintech" has been defined in various ways but encompasses a wide spectrum of technological innovations which impact a broad range of financial and payment services. This context makes it easier for technology startups (i.e. fintechs) to enter the financial services industry and offer products and services directly to consumers, businesses, and financial institutions (FIs).

FIs are increasingly investing resources in innovation. As fintech continues to evolve, industry stakeholders, both incumbent organizations and new entrants, should think broadly about this dynamic landscape to ensure that their offerings add value for consumers, investors, and markets in a manner that is safe, transparent, and sustainable. Government organizations should view their role as helping to create

[1] Regulators who attended the MPIW meeting represented the Federal Reserve Board of Governors ("FR Board") Division of Consumer and Community Affairs and Division of Supervision & Regulation; U.S. Department of Treasury (Treasury); Federal Deposit Insurance Corporation (FDIC); Office of the Comptroller of the Currency (OCC); Consumer Financial Protection Bureau (CFPB); National Credit Union Administration (NCUA); Conference of State Bank Supervisors (CSBS); and the Federal Trade Commission (FTC).

[2] The MPIW met previously with the regulators in April 2012 and May 2014. The summaries from these meetings are available at https://www.bostonfed.org/publications/mobile-payments-industry-workgroup/the-us-regulatory-landscape-for-mobile-payments.aspx and https://www.bostonfed.org/publications/mobile-payments-industry-workgroup/update-on-the-us-regulatory-landscape-for-mobile-payments.aspx.

a thriving, sustainable financial services environment that supports innovation and furthers other policy objectives, while working collaboratively with fintech innovators to mitigate potential risks.[3]

Fintech solutions that leverage digital and mobile channels have the potential to expand and improve access to financial products and services to all consumers, including the underserved. Although they are third party service providers or vendors and are expected to comply with relevant federal and state banking regulations, navigating the federal and state regulatory environment is complex. The MPIW and regulators discussed how stakeholders can work collaboratively to achieve the common goal of responsible innovation and provide guidance and education for the fintechs and their FI partners, who are responsible for ensuring that fintechs comply with relevant regulations.

U.S. regulators are aware of the need to become more fintech friendly. In March 2016, the Office of the Comptroller of the Currency (OCC) published a paper on responsible innovation in the federal banking system.[4] The OCC defines "responsible innovation" as the use of new or improved financial products, services, and processes to meet the evolving needs of consumers, businesses, and communities in a manner that is consistent with sound risk management and is aligned with the bank's overall business strategy. The paper discusses the principles that will guide the development of their framework for evaluating these services.[5]

In December 2016, the OCC published a proposal to develop a special purpose national bank charter to enable interested fintechs to apply for bank charter status. [6] This paper was available for comment through the end of January 2017. It outlines the OCC's authority to grant such charters and the potential minimum supervisory standards for successful fintech bank applicants. The OCC requirements are based on its expectations of a responsibly managed organization; therefore, it proposes a special purpose bank charter, not a "fintech" charter. The OCC does not seek to regulate technology but to regulate companies that provide *banking services* as defined under the National Banking Act.[7] These requirements are no

---

[3] U.S. National Economic Council (2017, January). *A framework for fintech*. The White House. Retrieved from https://obamawhitehouse.archives.gov/sites/obamawhitehouse.archives.gov/files/documents/A%20Framework%20for%20FinTech%20_FINAL.pdf.

[4] U.S. Office of the Comptroller of the Currency. (2016, March). *Supporting responsible innovation in the federal banking system: An OCC perspective*.

[5] The OCC also recently released a Supplement to explain how it will apply the licensing standards and requirements in its existing regulations and policies to fintech companies applying for a special purpose national bank charter. OCC (2017, March). *Comptroller's licensing manual draft supplement*, available at https://www.occ.gov/publications/publications-by-type/licensing-manuals/file-pub-lm-fintech-licensing-manual-supplement.pdf.

[6] U.S. Office of the Comptroller of the Currency. (2016, December). *Exploring special purpose national bank charters for fintech companies*.

[7] The National Bank Act of 1863 was designed to create a national banking system, float federal war loans, and establish a national currency. Congress passed the act to help resolve the financial crisis that emerged during the early days of the American Civil War (1861–1865). See https://www.gpo.gov/fdsys/pkg/USCODE-2011-title12/pdf/USCODE-2011-title12-chap2-subchapI-sec38.pdf.

different than those followed by other banks with charters where the regulated entity provides banking services. The OCC's Innovation Office will be the initial point of contact for companies interested in becoming banks and the applicability of requirements will depend on how the company operates those banking services.

Payment industry stakeholders voiced their concerns about the inclusion of fintech companies in the federal banking system. Some did not see the need for a new charter and suggested that new institutions be subject to the same supervision and regulation as community banks and other types of FIs. Others emphasized the need to apply existing rules and oversight evenly and fairly. While fintechs can provide significant benefits of financial innovation to consumers and the industry, stakeholders affirmed that the innovations must be delivered responsibly.

Another issue with the OCC proposal is the potential $2 million minimum capital requirement for fintechs. If the capital requirement level is too high it could prevent entry by smaller startup companies that struggle just to meet minimum state level requirements, or limit them to only seeking partnerships. The OCC seeks to help fintechs, but to have entry into the banking system an entity must have a viable, sustainable business plan and be self–funding, which includes an appropriate level of capital.

Meeting participants also noted that some of the rules created for traditional banks are outdated and not applicable to startups. Some suggested that fintech companies need to be bank-friendly and speak the language of financial services, and that holding fintech companies to banking standards may avoid wasteful investments. The challenge is how to strike a balance between necessary regulation of fintechs and not impeding innovation. Regulation should evolve with technology and changing customer preferences, although the group agreed that financial service regulators may not be technology experts or strategists.

II. Regulatory Framework for Mobile/Digital Wallets

MPIW members and regulators also discussed current mobile and digital wallet developments. Some regulators raised concerns that the number of solutions and different technology platforms (e.g., near field communication (NFC),[8] cloud, QR code) in the market create fragmentation, and possibly increase risk. They also highlighted consumer protection issues related to data ownership.

[8] Near-field communication (NFC) is a standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart.

The mobile phone has become a very powerful device, yet consumers do not fully understand the extent of its capabilities. The proliferation and accessibility of mobile apps have enabled consumers to easily download many apps to their mobile phones. It is likely that they do not regularly use all the apps and more importantly, do not understand how the apps use their personal data. For example, they have a tendency to opt-in to share their data with a merchant or wallet provider. Consumers may worry less about the risks of sharing their personal data because they can rely on current protections under Reg. E[9] or their FIs to make them whole in the event of unauthorized use. They may be unaware of the consequences when granting permissions to a mobile wallet or mobile app provider to access data on the mobile device, which can include permission for the provider to retain and use the data for marketing purposes, and even to track the consumer when an app is closed. Even if wallet providers only collect data to help perform risk management, they need to balance the amount of data collected with consumer privacy.

Dispute resolution is another area of concern. The way in which wallet providers handle consumer payment problems is not consistent and sometimes unclear on who to contact if there is a problem with an underlying funding source in the mobile wallet (e.g., issuing bank, wallet provider, merchant). Wallet solution providers and merchants may have different guidelines in their terms and conditions or user agreements that inform consumers how to resolve issues or payment disputes so should be explicit in describing their dispute resolution processes and contact information.

Reg. E also comes in to play for wallet payments funded with a debit card under its "access device" requirement. Contactless devices (e.g., mobile phones) used to initiate debit card transactions processed over existing payment card networks are considered access devices. However, some wallet providers are not aware of this Reg. E requirement and that they must comply with its provisions.

From a regulatory perspective, FIs partnering with mobile/digital third party solution providers need to perform due diligence to ensure that the third parties follow the rules for data protection, privacy, and dispute resolution. When consumers have problems they are more likely to contact their FIs, who realize most of the responsibility for addressing disputes.

III. European Union (EU) Payment Services Directive 2 (PSD2)

[9] The Electronic Fund Transfer Act (EFTA) (15 U.S.C. 1693 *et seq.*) of 1978 is intended to protect individual consumers engaging in electronic fund transfers (EFTs) and remittance transfers. The EFTA is implemented through Regulation E, which includes official interpretations. For more information, see https://www.federalreserve.gov/boarddocs/supmanual/cch/efta.pdf.

Many other developed countries and/or regions (e.g., Australia, Canada, EU, and UK) are more proactive in managing and directing their payments initiatives in the areas of standards and regulations. In 2007, the European Banking Authority (EBA) introduced the Payments Services Directive I (PSD1) to create a legal framework for payments across the EU that would foster efficiency and innovation. This prompted some EU non-bank companies to offer new middleman services to consumers, merchants, and FIs. The FIs objected to these new services that held consumer credentials and had access to FI consumer data.

The government (i.e. European Commission, European Parliament, and European Council) intervened with the introduction of Payment Services Directive II (PSD2).[10] PSD2 created a new class of players in the payments ecosystem, payment initiation service providers (PISPs) and account information service providers (AISPs). It requires Europe's banks to offer third-party providers greater access to customer data and payment infrastructure. To provide this access, banks will most likely have to use application programming interfaces (APIs) because APIs offer a standardized interface and allow companies to adopt a modular approach for quickly and cost-effectively creating and scaling new businesses.[11] PSD2 has acknowledged the need for security controls around access to these open APIs that allow third parties and merchants to access consumer bank accounts. PSD2 participants also realize that there is a lot of work involved in using APIs.

"Open API" can be interpreted widely across the industry. For example, some APIs are considered open because they are non-sensitive, but other services must be regulated or vetted because unqualified entities should not be able to access transaction data. "Open" does not refer to "wide open" or "unsecure;" a better description might be "external" APIs to distinguish from web services that are only available within FIs.

PSD2 also requires an unconditional right of refund to consumers for direct debits and strong (risk-based) authentication for all electronic transactions initiated by a payer, except those under a certain monetary threshold.[12] However, some industry stakeholders were concerned that the draft rules for strong customer authentication would greatly inconvenience customers and pushed back on this requirement in the draft

[10] PSD2 principles stem from EU Commission regulation, but the European Banking Authority determines the business rules, or the Regulatory Technical Standards (RTS), on areas such as authentication. The EU market is expected to be PSD2 compliant by January 2018, although the RTS rules are not expected to be in effect until November 2019.

[11] PSD2 was also designed to promote competition in payments, increase payment transaction security, improve the customer experience, promote integration of European payment markets, and enhance customer protection with payment and security innovation.

[12] Strong customer authentication is defined as "authentication based on the use of two or more elements categorized as knowledge (i.e. something only the user knows), possession (i.e. something only the user possesses), and inherence (i.e. something the user is). These elements must be independent so that breach of one element does not compromise the reliability of the others." See https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2. For further details refer to the EBA Final Draft Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) and Common and Secure Communication under PSD2.

Regulatory Technical Standard (RTS), underscoring that one-size does not fit all and some businesses are inherently riskier than others. They also noted that the requirements were too narrow and prescriptive and would hamper the development of e-commerce in Europe. The draft guidance could create disproportionate barriers for customer authentication, stifling the development of the e-commerce sector in Europe. AISPs and PISPs may create disintermediation by unbundling the payment service, making it more difficult for the FI to help resolve problems and for customers to know where to seek help.

The MPIW and panelists agreed on the importance of considering the lessons learned from the development of the PSD2 and potential impacts to the U.S., although merchants voiced concerns about being too prescriptive.

Lessons learned from PSD2 and potential applicability to the U.S. included:

1. Start with the consumer focus. The urgency to develop PSD2 overlooked the need to address consumer impacts.
2. Engage public and private sectors collaboratively sooner rather than later. PSD2 did not initially consider private sector feedback which delayed needed collaboration between both sectors.
3. Payment methods and types of purchases are not the same, i.e. one-size does not fit all. Allow for differences in developing the requirements.
4. Avoid unrealistic legislation because there is no silver bullet to eliminate fraud (i.e. zero fraud cannot be achieved). Instead, establish fraud targets for stakeholders using real-time systems.
5. Avoid overly prescriptive standards which create advantages for fraudsters by identifying specific solutions to attack.
6. Use hard data to evaluate issues.
7. Develop practical, achievable solutions.
8. Carefully consider what the requirements should be and create standards across FIs and countries.

IV. Conclusions

No major surprises emerged from the discussions with the regulators, but the MPIW identified several issues and opportunities for further analysis.[13]

1. Fintechs should leverage avenues available through the OCC and CFPB[14] to receive guidance as they develop new solutions.

[13] These conclusions do not reflect the opinions of the regulatory agencies represented at the meeting.

2. Disintermediation is trending with the involvement of multiple parties, which makes the payment process more complicated for consumers and other stakeholders.

    - Regulators' authority over third parties through the Bank Service Company Act (12 USC 1861, et seq.) has not been revised since the 1980s and does not consider today's environment. This law should be reviewed and updated.

3. Consider developing standards or best practices to modernize the payments ecosystem focused on mobile payments, NFC, and other mobile payment technologies.

4. Monitor the payment activities in other developed countries, including the EU/PSD2 to understand similarities in the issues they are addressing and the applicability of those regulations/standards to the U.S.

5. All stakeholders (FIs, processors, retailers, mobile/digital wallet solution providers, mobile network operators (MNOs), and regulators) share responsibility in managing the risks associated with mobile payments.

6. Education plays a key role for all stakeholders and consumers but needs to be tailored to each industry. All participants would benefit from education on the new wallets and underlying security technologies (e.g., encryption, payment tokenization), but regulators, in particular, need education on various aspects of mobile/digital payments before they can consider whether a potential issue needs to be addressed. Fintechs clearly need a better understanding of their role in the regulatory environment, Reg. E, and their consumer protection and data responsibilities, particularly if the wallet providers offer money movement from an FI or stored value accounts.

[14] See U.S. Bureau of Consumer Financial Protection (2016, Oct. 24) *Project Catalyst report: Promoting consumer-friendly innovation*, which highlights the importance of ensuring consumer protections are built into emerging products and services from the outset. Also, CFPB (2016, Feb. 2). *Policy on No-Action Letters; information collection* and CFPB trial disclosure program: https://www.consumerfinance.gov/about-us/project-catalyst/trial-disclosure-program/. Much federal consumer protection law rests on the assumption that accurate and effective disclosures will help Americans understand the costs, benefits, and risks of different consumer financial products and services.