Mobile Payments Industry Workgroup | December 3, 2019

Regulatory and Payments Industry Stakeholder Perspectives: Fintech Innovation, Privacy, Open Banking, and Secure Payments

MPIW June 2019 Meeting — Summary of Key Findings

Susan Pandy, Ph.D. and Marianne Crowe

The Mobile Payments Industry Workgroup (MPIW)[1] meets with representatives from federal and state regulatory agencies[2] every 2-3 years to gauge their level of involvement in the mobile/digital payments industry and engage in dialogue with industry experts on developments, challenges, and potential gaps where agencies can add value.[3] Topics discussed at the June 2019 MPIW meeting included: how U.S. regulatory agencies are supporting financial technology (fintech) developments, potential changes to U.S. privacy and consumer protection laws for mobile/digital payments, open banking, authentication, and mobile payments in the fuel industry.

The views expressed in this paper are those of the author and do not necessarily represent those of the Federal Reserve Bank of Boston or the Federal Reserve System.
Mention or display of a trademark, proprietary product, or firm in this report does not constitute an endorsement or criticism by the FRBB or the FRS and does not imply approval to the exclusion of other suitable products or firms.

1 The Federal Reserve Banks of Boston and Atlanta convene the MPIW. See https://www.bostonfed.org/about-the-boston-fed/business-areas/payment-strategies.aspx.

[2] Regulatory agencies represented included: Federal Reserve Board Division of Consumer and Community Affairs and Division of Supervision and Regulation; U.S. 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); Federal Trade Commission (FTC); and the Federal Communications Commission (FCC).

[3] The MPIW previously met with regulators in January 2017, May 2014, and April 2012. See meeting summaries at https://www.bostonfed.org/publications/mobile-payments-industry-workgroup/whats-new-with-regulation-in-the-mobile-payment-and-Fintech-space.aspx; 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.

I. Fintech Developments and the Regulatory Environment

A 2019 KPMG study reported that fintech investment in the U.S. hit a record $52.5 billion in 2018.[4] Fintech is rapidly transforming the financial services industry, requiring financial institutions (FIs) and regulators to understand the impacts to operations, regulation, security, and customer experience. Fintechs seek to add value across the payments value chain by embedding payments into technology applications that improve efficiencies and address gaps.

As fintech innovation continues to thrive, both federal and state regulatory agencies are using a broad range of approaches to embrace new technologies. The approaches include offering special purpose charters to non-bank technology companies, publishing guidance, creating fintech-focused work groups, and creating opportunities for partnerships. Financial institutions are also assisting fintechs through partnerships to help address regulatory challenges.

The first panel discussed regulatory, consumer advocacy, and industry perspectives on fintech and innovation developments. The Office of the Comptroller of the Currency (OCC) and Federal Deposit Insurance Corporation (FDIC) representatives shared their perspectives on innovation. The National Credit Union Administration (NCUA) discussed the opportunities and challenges for credit unions to engage with fintechs. The National Consumer Law Center (NCLC) expressed the need to consider consumer protection, and Radius Bank discussed its role as a virtual bank and partner to many fintechs.

Federal Agency Approaches to Fintech and Innovation in Mobile Banking and Payments

The OCC regulates nationally chartered banks, federal savings associations, and federal branches of foreign banks operating in the U.S. It also focuses on emerging technology trends and fintech by conducting outreach and market analysis. The OCC takes a cross-functional approach that spans the supervision, economics, legal, and policy divisions of the agency. This analysis allows the OCC to provide timely information about technology and trends to FIs, fintechs, and internal OCC examiners. In this capacity, the OCC's Office of Innovation works with stakeholders across the federal banking system and coordinates efforts across the agency.

The OCC's plan to offer a special charter began when fintech companies sought to engage in banking on a national scale. The OCC has several chartering options including full-service, trust, and special-purpose charters. Full-service charters include insured deposits (which require FDIC insurance), and special-purpose charters cover entities that are engaged in a core banking activity, but do not plan to accept deposits.

[4] KPMG (2019). *The Pulse of Fintech – H2 '18: Biannual Global Analysis of Investment in Fintech.* Available at https://home.kpmg/xx/en/home/insights/2019/01/pulse-of-Fintech-h2-2018.html.

The OCC supports "responsible innovation," or the development of safe and secure financial products that meet the evolving needs of consumers and businesses. OCC staff is available to FIs and businesses to connect for assistance. The agency often meets with fintechs to help them understand how to operate in the regulatory environment and to discuss their innovation strategies and consumer needs.

The FDIC efforts to support innovation include the launch of the FDIC Tech Lab (FDiTech) to promote the adoption of innovative technologies across the financial services sector. FDiTech will engage bankers, fintechs, technologists, and other regulators on innovations; conduct "tech sprints,"[5] and pilot projects to test emerging technologies in cooperation with states and affected federal regulators. It will also support and promote the adoption of new technologies by FIs, particularly at community banks and expand banking services to the unbanked, underbanked, and individuals in underserved communities through new technologies. The FDIC is also considering strategies for new regulatory technology (reg-tech)[6] and supervisory technology (sup-tech)[7] solutions.

To increase the transparency of the deposit insurance application process for new FIs, the FDIC published a handbook and released the applications-related procedures that guide the FDIC's review and processing of applications.[8] The FDIC also established a process that allows prospective applicants to submit draft deposit insurance proposals in order to obtain FDIC feedback, which can be used to strengthen the formal application. These initiatives help organizers become familiar with and navigate the application process.

Innovation and technology also have the potential to advance the ability to reach unbanked and underbanked consumers, an area of focus for the FDIC. For example, the FDIC's most recent biennial survey of underbanked and unbanked households showed that an increasing proportion of consumers use mobile banking to access their bank accounts. The proportion of banked households that used mobile banking to access their accounts in the past 12 months increased from 23.2 percent in 2013 to 40.4 percent in 2017. The share of banked households that used mobile banking as their *primary* method of account access also increased sharply from 2013 to 2017, both overall and across household characteristics.[9] While branch banking continues to be important for many households, qualitative research reflects the opportunities that mobile financial services present for financial inclusion.[10]

---

[5] Tech sprints are typically two-day events that bring together participants from across and outside of financial services to develop technology-based ideas or proof of concepts to address specific industry challenges.
[6] Reg-tech is a class of software apps for managing regulatory compliance. Companies invest in reg-tech as a way to save time and resources.
[7] Sup-tech is technology for the regulators themselves. As with other reg-tech, it focuses on improving efficiency through the use of automation, introducing new capabilities, and streamlining workflows. By digitizing data and allowing the computing power to perform checks, keep tabs, and systemize the processes, sup-tech can enable better reporting, oversight, and overall compliance for regulators.
[8] Federal Deposit Insurance Corporation. (2017, April). *Applying for Deposit Insurance*. *A Handbook for Organizers of De Novo Institutions.* Available at https://www.fdic.gov/regulations/applications/handbook.pdf.
[9] FDIC (2017). 2017 *FDIC National Survey of Unbanked and Underbanked Households*. Retrieved from https://www.fdic.gov/householdsurvey/2017/2017report.pdf.
[10] See economicinclusion.gov for survey findings.

The National Credit Union Administration (NCUA) charters and insures credit unions and is monitoring fintech developments. It has established a fintech working group that explores how credit unions can adopt and embrace fintech and overcome barriers, such as the competitive disadvantage that fintechs may pose to credit unions. Credit unions are interested in understanding how new technology can create value and differentiation as well as enhance their member experience. Many credit unions are seeking collaboration and partnerships with fintechs as a way to move forward in this changing technology environment, but they also have concerns from a competitive standpoint.

The NCUA is currently assessing creation of a program to support innovation and working with credit unions to help them make it successful.

Fintech and Innovation at the State and Consumer Level

For the Conference of State Bank Supervisors (CSBS), regulation is activities-based and does not change for fintechs. Fintech activities fit within existing state regulations, such as the state money transmission laws. In 2017, the CSBS created Vision 2020, a set of initiatives aimed at harmonizing multi-state regulation. Under Vision 2020, regulators sought input from fintechs on how to streamline regulation across the country. As a result, the CSBS is developing a model state payments law for money transmitters. This law will provide more consistency between state licenses and multi-state efforts, reducing some inefficiencies for multi-state companies.

The National Consumer Law Center (NCLC) discussed the importance of consumer protection relevant to emerging fintech developments, emphasizing that new products such as person-to-person (P2P) payments and faster payments may have unintended consequences or risks. The reliance of fintech on mobile and internet-based platforms and electronic communications may disadvantage consumers more suited to physical customer service or those who do not own smartphones. Furthermore, the industry needs to be aware of fintech companies' collection and use of consumer data and the potential lack of transparency.

The NCLC wants companies to provide safe and secure technology for consumer payment products. It is not convinced that P2P mobile payments provide sufficient security to protect consumers from fraud and errors. Finally, the organization prefers the state legal model versus the use of charters, and it supports pilot testing over the use of fintech sandboxes.[11]

Partnerships between FIs and fintechs present an alternative to fintech charters for some companies. Radius Bank supports the option for fintech charters but prefers working through partnerships. Many fintechs excel at creating new products that offer consumers more innovative services. These

[11] For more information on the NCLC's perspectives on Fintech, see National Consumer Law Center (2019, March). *Fintech and Consumer Protection: A Snapshot*. Available at https://www.nclc.org/images/pdf/cons-protection/rpt-Fintech-and-consumer-protection-a-snapshot-march2019.pdf.

companies recognize the value of working with a bank partner, such as Radius, which understands the regulatory community and requirements.

Panelists noted that the industry must include security tools to guard against fraud as new payment methods are introduced, such as mobile P2P and faster payments. Not all stakeholders agree that the necessary fraud control measures are available to provide adequate authentication of all parties to a transaction. This is an industry-wide problem where industry collaboration can more effectively address greater mobile fraud risk by leveraging the experience and knowledge of current fraud prevention approaches in the areas of biometrics and artificial intelligence (AI) (e.g., neural networks, deep AI, and machine learning). All of these approaches can help to detect fraud and identify major attacks before they occur.

II. U.S. Data Protection and Privacy Developments

With the rapid pace of mobile and digital innovation occurring across the financial services landscape, the need to protect the privacy of consumers and their data has become more important. It is difficult to achieve this goal at a national level because the U.S. is comprised of a patchwork of federal and state regulations.

In June 2018, the California Consumer Privacy Act (CCPA) became law and goes into effect as of January 1, 2020. Currently, it is the strongest privacy legislation enacted in any state in the U.S., giving more power to consumers to control their private data, although it does not match all of the protections enacted by the European Union (EU).[12] Panelists, representing the Federal Trade Commission (FTC), Consumer Reports, CTIA,[13] and the Federal Communications Commission (FCC), discussed their perspectives on CCPA and its impact to industry stakeholders, particularly those in the mobile/digital payments environment, and the potential for a national privacy law.

The still-evolving CCPA, increases transparency by allowing consumers to request data that has been collected about them, in a readily usable format (e.g., electronically) free of charge.[14] The law applies to businesses that collect, sell, or share consumer data. CCPA does not declare any data collection or sharing off-limits, but it allows consumers to opt out of selling their data with certain nuances (very limited right of action)[15] and provides deletion requirements.

The FTC is the authoritative agency for privacy and data protection and supports the need for national privacy laws. Under the FTC Act, the agency has authority over unfair, deceptive, or abusive acts

[12] In contrast to the U.S., the GDPR provides a comprehensive framework for privacy protection that covers all EU countries and harmonizes data protection regulations across the EU. This harmonization brings much-needed certainty to regulators, businesses, and consumers.
[13] CTIA represents the U.S. wireless communications industry. For more information, see https://www.ctia.org/.
[14] Data portability means that the consumer can request their information and have it delivered by mail or electronically - in a portable and readily useable format that allows the consumer to transmit this information to another entity without hindrance.
[15] The opt out of sale law does not allow companies to discriminate against consumers who opt out of allowing their data to be sold, but they can charge the consumers differential pricing, which raises questions about data as currency.

and practices (UDAAP) in or affecting commerce.[16] The agency held hearings in 2018 and 2019 to discuss the rapid pace of innovation and its impact on consumer privacy, data security, emerging technologies, as well as broader issues and developments that could affect U.S. consumer protection laws.[17] The hearings flagged several privacy issues, such as when consumers need notice and choice about how businesses collect and use their information; and whether consumers are capable of making intelligent choices about privacy, given the information available to them.

The CCPA also covers information sharing but wants consumers to have meaningful choices to ensure that data is relevant to the purpose for which it was collected. Consumer Reports (CR) worked with other organizations to develop The Digital Standard, an open effort to create a digital privacy and security standard to help guide the future design of consumer software, digital platforms and services, and Internet-connected products. CR also works to pass strong privacy legislation and supported the CCPA. The organization agrees that practice of notice and choice lacks an option for meaningful consumer choice and it created categories of information that third parties collect about consumers. The EU's General Data Protection Regulation (GDPR)[18] privacy policies have struggled with providing meaningful choice to consumers.

The FTC states that businesses provide a "just-in-time" disclosure[19] before allowing third party apps to access sensitive content through application programming interfaces (APIs), such as geolocation information. They should obtain consent from consumers just prior to the collection of such information by apps, which will allow users to make informed choices about whether to allow the collection of such information. For example, a pop-up window could display a just-in-time notice for P2P payments to notify the consumer about the cost of the transaction and offer a less expensive option. Pop-up solutions could also work for privacy choices.

Understanding the extent of information that companies collect about consumers is very difficult and needs to be explained to consumers and the parties responsible for the data.

Regulatory Activities in the Mobile Service Provider Industry

Robocalls represent approximately one-half of all calls and create operational costs and customer service issues to businesses that prefer not to manage the complaints.[20] The Federal Communications Commission (FCC) representative discussed its initiatives to address robocall

---

[16] Section 5 of the FTC Act, 15 USC 45(a) (1) (UDAAP), prohibits "unfair or deceptive acts or practices in or affecting commerce."
[17] U.S. Federal Trade Commission (2018). *Hearings on Competition and Consumer Protection in the 21st Century*. Available at https://www.ftc.gov/policy/hearings-competition-consumer-protection.
[18] The GDPR (EU) 2016/679 is an EU regulation on data protection and privacy for all individual citizens of the EU and European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. Its primary aim is to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.
[19] Federal Trade Commission (2012, March). *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers*, Supra note 2, at 60.
[20] A robocall is a phone call that uses auto-dialing technology to deliver a pre-recorded message with product offers or attempts to steal personal information that could later be used to commit payments fraud.

problems and tools to block or eliminate them. In June 2019, the FCC passed a new rule to allow mobile network operators (MNOs) and service providers to block robocalls as a default, automatically opting customers in to the service. Customers can choose to opt out of blocking services offered by the MNOs. Some service providers currently offer call-blocking tools, but mobile phone subscribers must opt in to use them.

In November 2018, the FCC requested that the phone industry adopt a robust call authentication system to combat illegal caller ID spoofing by the end of 2019. In June 2019, the FCC adopted a Notice of Proposed Rulemaking,[21] enabling the agency to mandate implementation of the SHAKEN/STIR caller ID authentication framework[22] if the year-end deadline is not met. As calls are routed, the caller number or caller ID is verified to determine that it is legitimate and not spoofed. The proposed rulemaking does not cover call content nor does the authentication method verify if the number is fraudulent, but it does help reduce fraud associated with calls and spoofing.[23]

III. Developments in Open Banking and APIs

Open banking allows for the secure transmission of account data authorized by the customer to a third party service provider (TPP), chosen by the customer. Financial institutions offer TPPs access to online banking accounts and financial services via APIs, which provide a standard format for information transfer, secure data sharing, and applications.

The use of APIs enables a wide variety of new services. Third party collaboration can lead to new product development that can enhance the overall consumer financial experience. For example, TPPs can access a consumer bank account for a certain period to review the customer's money management and possibly recommend a new financial product. Similarly, the FI or TPP may alter its approach to loan approvals by collecting information about a consumer's financial habits (e.g., bill payment, savings history) rather than or in addition to assessing credit scores.

Customer consent is mandatory to information sharing in an open banking environment. Ownership of the data and its use is a critical issue. Many bank customers claim ownership of their data and the right to access it. They have concerns about privacy and want to share in the management of their data, particularly related to mobile.

Globally, open banking projects seek to increase competition and improve services for end users. This panel[24] explored lessons learned from the U.K.'s open banking initiative driven by the Payment

[21] U.S. Federal Communications Commission (2019, June 7). *Declaratory Ruling and Third Further Notice of Proposed Rulemaking*. Retrieved from https://docs.fcc.gov/public/attachments/FCC-19-51A1.pdf.
[22] SHAKEN/STIR are acronyms for Signature-based Handling of Asserted Information Using Tokens (SHAKEN) and the Secure Telephone Identity Revisited (STIR) standards. SHAKEN/STIR digitally validates the handoff of phone calls passing through the complex web of networks, allowing the receiving consumer's phone company to verify that a call is from the person making it.
[23] For more information, see https://www.fcc.gov/call-authentication.
[24] This panel included a representative from the U.K., and representatives from the Consumer Financial Protection Bureau and the Federal Reserve Board of Governors.

Services Directive II (PSD2)[25] and compared this to initiatives in the U.S. Panelists also discussed the overall value and challenges to open banking.

Unlike the U.K., U.S. bank regulatory agencies have not issued any new regulations to support open banking. The U.K. offers a useful test bed for open banking and lessons to other countries seeking to adopt it.

U.S. regulatory agencies acknowledged that there is a market and some demand for open banking. However, they expressed the need for a regulatory framework that provides consumer protection. For example, the EU's PSD2 mandates Strong Customer Authentication (SCA) for online banking services and for initiating and processing electronic payments. It also requires TPPs to be licensed, insured, and registered in an open banking directory. The U.S. does not have similar protections, so TPPs may not be fully vetted. As a result, FIs are responsible for any financial losses and data theft.

Opening a bank's platform to third party applications can create synergies with innovative technology businesses to build a new generation of digital customer experiences that are convenient and advantageous. However, an API-driven system will require FIs to manage large data requests and also detect and prevent fraud. Open banking also raises concerns around privacy and access to consumer data, including whether consumers understand how their data is shared and securely deleted. Trust is a critical success factor for open banking. A key driver to building trust is ensuring data is not lost or stolen, and that it is only used for the purposes for which customers grant permission.

Regulatory Perspectives on Open Banking and APIs

The Consumer Financial Protection Bureau (CFPB), U.S. Treasury, and the Federal Reserve Board are active on several fronts. In 2017, the CFPB published *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* to address security, privacy, and informed consent, among other topics.[26] The agency has included the topic of consumer access to financial records as part of its long-term rulemaking agenda and plans to organize a symposium on consumer-authorized data sharing. In 2018, the U.S. Treasury issued *A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation* with comparisons on open banking and faster payments.

[25] PSD2 is a data and technology-driven directive that aims to drive increased competition, innovation, and transparency across the European payments market, while also enhancing the security of Internet payments and account access. At the core of PSD2 is the requirement for banks to grant third party providers access to a customer's online account/payment services in a regulated and secure way.

[26] U.S. Consumer Financial Protection Bureau (2017, Oct. 18). *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*. Available at https://www.consumerfinance.gov/data-research/research-reports/consumer-protection-principles-consumer-authorized-financial-data-sharing-and-aggregation/.

In 2017, Federal Reserve Board Governor Lael Brainard spoke publicly on the role of FIs in the fintech stack and how the U.S. thinks about these issues.[27] While there are many benefits from allowing access to the bank technology stack, her remarks supported earlier comments about clarifying ownership and use of consumer data. Other considerations included third party relationships and dependencies (i.e., build or buy), and whether to partner with fintechs or offer fintech charters. These considerations require evaluation and modernization of agency guidance on rules for third party risk management.

U.S. regulatory agencies view education as an important facet of open banking to ensure that consumers truly understand the significance of data aggregation, retention, and reuse by TPPs.

Trust between all parties engaged in open banking needs examination. This includes a review of risk management requirements between FIs, TTPs and data aggregators, transparency, effective customer protections, and clear ownership of liability. Parties also need to prepare customers for a potential increase in phishing, robocalls, and other fraud attempts.

Regulation E[28] generated consumer trust for electronic payments by limiting a consumer's liability for unauthorized debit card transactions, as well as providing other protections. A shift towards open banking and the introduction of TPP intermediaries between FIs and consumers could require a review of the liability ownership. The CFPB issued its consumer principles to encourage the private sector to protect the interests of the consumer.

Another concern with open banking is whether TPPs help or hinder smaller FIs, which typically use TPPs to develop APIs and other financial tools. One suggestion was for regulators to address large TPPs and new providers through their oversight role by developing good relationships and performing strong TPP testing.

U.S. regulators have become more open to meeting with industry stakeholders they do not regulate to discuss open banking. They are hiring more staff with industry experience to have a better understanding of payments beyond banking. The agencies also work together to coordinate their messaging on this topic.

---

[27] U.S. Federal Reserve Board of Governors (2017, April 28). *Where Do Banks Fit in the Fintech Stack?* [Speech by Federal Reserve Board Governor, Lael Brainard]. Retrieved from https://www.federalreserve.gov/newsevents/speech/brainard20170428a.htm.

[28] Regulation E was issued by the Bureau of Consumer Financial Protection pursuant to the Electronic Funds Transfer Act (EFTA) and establishes the basic rights, liabilities, and responsibilities of consumers who use electronic fund transfer and remittance transfer services and of financial institutions or other persons that offer these services. The primary objective of the act and this part is the protection of individual consumers engaging in electronic fund transfers and remittance transfers.

Open Banking and Standard API Efforts in the U.S.

The Financial Data Exchange (FDX)[29] and the National Automated Clearing House Association (NACHA)[30] have initiatives to advance open banking. FDX has aligned a cross-section of FIs, fintechs, and financial services groups around a single data-sharing standard to accelerate the adoption of open banking API frameworks and standardize the transfer of data. An industry-backed standard could replace all incompatible APIs and custom data-sharing arrangements. NACHA's API Standardization Industry Group is developing a tool for FIs, businesses, fintechs, and other industry stakeholders to support the payments and business needs of FIs, businesses, fintechs, and other industry stakeholders.

Open Banking in the U.K.

The deadline to comply with the U.K. open banking regulation was January 2018. Based on industry research, few consumers in the U.K. understand open banking. A 2018 survey by Unlimited Group revealed that while nine percent of U.K. adults have used an API-initiated app or service, only 22 percent have heard of open banking.[31] Furthermore, concerns over data security, breaches, and privacy resulted in an overall lack of trust in open banking. The study also noted that the most commonly used apps are those that allow users to view accounts from different financial suppliers in one place or help consumers save or invest. Apps that enable consumers to switch financial providers or give consumers control of their data were not widely used (both one percent).

Despite the slow start, some efforts have been successful. For example, Barclays strongly marketed the benefits of open banking to its mobile banking customers. When customers check their mobile banking accounts (typically once per day) a message is displayed that asks them if they want the bank to manage their accounts from other banks. Currently, Barclays has over 7 million users.[32]

IV. Mobile/Digital Payment Authentication

The online identity authentication environment is growing quickly. Effective identity verification remains one of the greatest challenges facing payment industry stakeholders. EMV chip cards have made the point-of-sale environment more secure by reducing fraud, shifting it to the online environment. To make e-commerce more secure, several authentication protocols are active:

---

[29] For more information, see https://financialdataexchange.org/.
[30] NACHA is a nonprofit organization that convenes hundreds of diverse organizations to enhance and enable ACH payments and financial data exchange within the U.S. and across geographies. See www.nacha.org.
[31] Unlimited Group. (n.d.). *Open Banking: A Revolution Stalled.* 2nd Ed. Retrieved from https://www.unlimitedgroup.com/wp-content/uploads/2018/12/LG-Unlimited-Open-BankingReport_Splendid_v03_LR.pdf.
[32] Barclays (2019, April 26). *How Barclays is Leading the Way with Open Banking*. Retrieved from https://home.barclays/news/2019/04/how-barclays-is-leading-the-way-with-open-banking/.

EMVCo[33] Secure Remote Commerce Specification (SRC spec),[34] EMV 3-Domain Secure (3DS),[35] the World Wide Web Consortium's (W3C) Webauthn,[36] and Fast Identity Online (FIDO) Alliance.[37]

This panel[38] discussed industry and regulatory perspectives on security and authentication approaches for mobile and remote payments. The panel noted the need to balance securely authenticating a user with convenience and privacy. The approaches share a common goal to provide more security and a better experience for consumers, issuers, merchants, and service providers, but questions about compatibility and interoperability between the approaches require further analysis.

EMVCo's Secure Remote Commerce Specification and 3DS 2.0

A growing number of merchants work with FIs, card networks, and multiple third party processors to enable customers to enter their payment card (or bank account) information into a merchant mobile app or website. The current environment lacks common integration models, practices, and specifications, creating fragmentation, complexity, and inconsistency. The purpose of the SRC spec is to create a standard e-commerce checkout method, based on a framework proposed by EMVCo in November 2017. The SRC spec enables a merchant to securely request and receive interoperable credit and debit card data from participating issuers to process remote commerce transactions.

The goal of SRC is to provide a seamless guest checkout solution. Mastercard worked closely with partners, merchants, and other stakeholders to ensure an efficient rollout, focusing on transparency and transaction security, including its authentication efforts with regulators to determine if any adjustments to regulations are needed. Commercial implementations of the SRC spec are currently underway in the market.

The SRC spec was designed to be compatible with the EMV 3DS 2.0. 3DS 2.0 performs risk-based authentication (RBA) in the background, only prompting for step-up authentication (e.g., one-time password, biometrics) for higher risk transactions, significantly reducing customer friction. Effective

---

[33] EMVCo is a global technical body that facilitates the worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV specifications and related testing processes. This includes chip-based payment cards, payment tokenization, and 3DSl. American Express, Discover, Visa, MasterCard, JCB, and Union Pay jointly own EMVCo.

[34] EMVCo (2019, June). *EMV Secure Remote Commerce Specification v1.0.* This specification describes how merchants can facilitate payment authorization for remote commerce transactions. It supports a streamlined process that works across channels, browsers, and devices and provides a consistent consumer checkout experience and common mark used by participating card networks and merchants. See https://www.emvco.com/terms-of-use/?u=/wp-content/uploads/documents/EMVCo-Secure-Remote-Commerce-Specifications-1.0.pdf.

[35] EMVCo's 3-Domain Secure (3DS) is a secure communication protocol that enables real time cardholder authentication from the card issuer to improve online transaction security and support the growth of e-commerce payments. It provides global interoperability and a consistent consumer experience across mobile app and browser-based channels and connected devices (e.g., Internet of Things). 3DS 2.0 functions separately from v1.0, which will phase out as 3DS 2.0 matures. 3DS 2.0 is currently being tested by FIs and merchants.

[36] The Webauthn specification describes an API to create and use strong, attested, scoped, public key-based credentials by web applications to provide strong user authentication.

[37] The FIDO Alliance develops specifications and certifications to enable an interoperable ecosystem of hardware-, mobile-, and biometrics-based authenticators to use with many apps and websites. See https://fidoalliance.org/.

[38] The panel was comprised of representatives from the CFPB, FTC, and Mastercard.

RBA should result in fewer than five percent of transactions needing step-up authentication, which will reduce issuer operational costs (e.g., call centers), accelerate the process, and increase transaction approvals.

The panel shared a concern raised by the European Banking Authority (EBA) opinion[39] that 3DS does not satisfy the inherence requirements for Strong Customer Authentication under PSD2 since the method of biometric authentication is not transmitted to the issuer.[40] While this requirement relates to the rollout of open banking in the EU, it is important to understand any potential gaps with 3DS for the U.S. Mastercard is working with its merchants and issuers to address uncertainty and prepare for SCA in Europe using 3DS, as well as biometrics.

Fast Identity Online Alliance (FIDO) and World Wide Web Consortium (W3C)

EMVCo collaborated with FIDO in two areas to leverage its authentication tools. First, it allowed the use of a FIDO authenticator as a consumer device cardholder verification method (CDCVM).[41] FIDO determined that its universal authentication framework (UAF) complied with the CDCVM requirements provided by EMVCo. Second, FIDO will include authentication in 3DS messages to the issuer. This will provide the issuer with new data that is cryptographically bound.

W3C's WebAuthn is a new global standard API for secure web authentication supported by all major browsers and platforms. WebAuthn allows a relying party, such as a web provider, to include strong authentication into its applications in all leading browsers and platforms. WebAuthn streamlines the ability to offer users strong authentication with a choice of authenticators, such as security keys, and built-in platform authenticators (e.g., fingerprint sensors). W3C also offers a Web Payment API, which allows a user to authenticate their enrolled credentials and preferred payment method. Once enrolled, the app can use WebAuthn as the credential.

W3C is leading a public interest group to coordinate the authentication efforts of EMVCo, W3C, and FIDO. It is working to develop complementary technologies to enhance the security and convenience of web payments.

---

[39] European Banking Authority (2019, June). *Opinion of the European Banking Authority on the Elements of Strong Customer Authentication under PSD2.* See Article 21: "…EMV 3DS 2.0 and newer would not currently appear to constitute inherence elements, as none of the data points, or their combination, exchanged through this communication tool appears to include information that relates to biological and behavioral biometrics…" Retrieved from https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf?retry=1.

[40] PSD2 defines SCA as an "authentication based on the use of two or more elements categorized as knowledge (something only the user knows); possession (something only the user possesses); and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed to protect the confidentiality of the authentication data."

[41] CDCVM evaluates whether the person presenting the payment instrument is the legitimate owner of the instrument. Apple Pay accepts Face ID, Touch ID, or the device passcode as the CDCVM, instead of the more traditional methods of PIN, signature for transactions in stores, or 3DS for transactions within apps.

CFPB and FTC Perspectives on Authentication

The CFPB is technology-neutral and does not consider itself an expert on how to build technology. Rather, it seeks background on emerging technologies and focuses that are results-oriented. The CFPB discussed the agency's broad consumer protection mandate, which addresses a variety of activities. The previously mentioned consumer principles focus on consumer control, transparency, trust, speed, and the availability of funds.

The CFPB conducts a biennial review of credit card practices, including security innovation. The August 2019 Consumer Credit Market Report includes feedback from issuers and an overview of where the industry stands in terms of security.

The activities of the CFPB and FTC can overlap, particularly in work related to non-banks. However, the agencies have a memorandum of understanding (MOU) that addresses areas of mutual interest, particularly for UDAAPs. The MOU allows the agencies to navigate any jurisdictional overlap and avoid undue burden to the companies they regulate. In addition to the MOU, the agencies have extensive, staff-level conversations and a shared database to avoid overlap and ensure the efficient use of resources.

The FTC has jurisdiction over non-bank lenders, app developers, and general retailers. The FTC addresses incidents where companies and FIs fail to employ adequate security measures. The Gramm-Leach-Bliley Act (GLBA) Safeguards Rule[42] establishes requirements for the information security programs of all FIs subject to FTC jurisdiction. The rule requires FIs to develop, implement, and maintain a comprehensive information security program. In early 2019, the FTC sought comment on several changes to the Safeguards Rule, including, for example, requiring encryption of customer information, both in transit and at rest; and implementation of multifactor authentication for any individual accessing customer information.

V. Payments in the Fuel Industry

The last panel[43] discussed the evolution of payments at the fuel pump, both from a retail and commercial perspective. Panelists noted challenges to the fuel industry related to meeting the EMV migration timeline and mitigating fraud. Related to mobile, the large fuel providers have developed full-feature apps that include a holistic consumer experience, including loyalty and rewards, location-based services, and other marketing information. Payments is only one component.

---

[42] U.S. Code of Federal Regulations (2002, May 23). *Part 314—Standards for Safeguarding Customer Information*. The Safeguards Rule requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure. In addition to developing their own safeguards, companies covered by the Rule are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care. Available at https://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=1e9a81d52a0904d70a046d0675d613b0&rgn=div5&view=text&node=16%3A1.0.1.3.38&idno=16.

[43] The panel was comprised of representatives from the Secure Technology Alliance, U.S. Bank, Cumberland Farms, and NCR Corporation.

Fuel industry providers prefer to have more customers interact with the pump, using their mobile phones to activate it, initiate the transaction, and pay for their purchase. This model reduces transaction time and friction, and increases security with a pre-enrolled bank account or payment card.

By capturing customer data, the fuel businesses can tailor the customer experience, expand offerings, and attract customers into their convenience stores as well. While some are considering contactless card payments, at locations that provide remote in-app functionality to activate the pump, it is not a priority; and many fuel businesses are still upgrading their automated fuel dispensers and software to accept EMV contact chip cards facing the liability shift deadline of October 1, 2020.

VI. Issues and Opportunities for Consideration

The MPIW identified several issues and opportunities for further analysis based on the meeting discussions.

1. Fintech and Innovation

- Partnerships between FIs and fintechs will play an important role in advancing fintech solutions and ensuring that fintechs understand the regulatory environment and consumer protection considerations.
- Fintechs should also develop relationships with regulators to facilitate communication and understand important compliance considerations.
- Credit unions and small to mid-sized FIs may be less knowledgeable of the fintech benefits and challenges and how fintech can help to enhance their customer relationships.
- Financial inclusion presents an opportunity for fintechs to develop solutions to meet the needs of the unbanked and underbanked populations.
- Mobile/digital payments are fueling innovation and fintech developments. However, the industry needs to ensure the safety and soundness of new payment methods that leverage mobile and to ensure adequate consumer education and protection.
- Developments to monitor include the evolution of limited charters, FI-fintech partnerships, and the impacts that the challenger/neo-banks will have on FIs and fintechs.

2. Privacy

- Industry stakeholders should continue to monitor the rollout of CCPA, forthcoming privacy laws in other states, and potential federal legislation and identify gaps and lessons learned as the U.S. moves toward a national privacy law.
- In particular, it will be important to understand how mobile payment apps protect consumer privacy.[44]

[44] The Clearing House. (2019, November). *Consumer Survey: Financial Apps and Data Privacy*. Retrieved from https://www.theclearinghouse.org/-/media/New/TCH/Documents/Data-Privacy/2019-TCH-ConsumerSurveyReport.pdf. This

3. Open Banking and APIs

- Continue to monitor open banking initiatives in other countries and, in particular, identify lessons learned.
- Identify and monitor developments in the U.S. and outline the benefits and challenges to an open banking regime.

4. Remote Payment Authentication

- Assess the value of new authentication approaches and tools for remote payments and how they can enhance fraud prevention and consumer protection.
- Monitor the implementations of EMVCo's SRC spec and 3DS to better understand the card networks' implementation requirements.

5. Regulation and Oversight

- What oversight role(s) will federal and state regulators play in fintech as the industry matures?
- How can the roles of federal and state agencies collaborate to avoid overlap?

VII. Conclusion

Fintech, or any innovation that relates to how businesses seek to improve the process, delivery, and use of financial services, is here to stay. Fintech will utilize emerging technologies such as AI, machine learning, and blockchain. Industry stakeholders and regulators need to accommodate this global phenomenon and adapt by adjusting their business strategies, developing new capabilities, and transforming their business models. Regulators are taking positive steps to improve relationships with the industry by sharing information, understanding emerging technologies, and conveying regulatory requirements.

At the same time, fintechs need to seek regulatory guidance and build trusted relationships with consumers and business partners to succeed. Trust will be a critical component to responsible innovation. Equally important will be general knowledge sharing between fintechs and regulators as an important part of enhancing the overall consumer experience.

A primary challenge for fintechs involved in the growth of mobile/digital payments is to ensure that they protect consumer information, and ensure that consumers understand what information is being collected about them and how it is being shared. Fintechs will need to be aware of potential regulatory developments at the national and state levels as consumer data rights become central to a digital economy.

---

study focuses on how non-bank financial apps access personal financial data and what consumers understand about these apps utilize the data.

Fintechs and other non-banks are also competing in the financial services industry by offering innovative ways to support mobile/digital payments. This is contributing to a paradigm shift in mobile payments, as consumers become more comfortable using digital wallets and the security, speed, and convenience that they provide. New authentication approaches may close security gaps in the remote channel and lead to increased consumer adoption.

The MPIW will continue to monitor this rapidly evolving payment environment and provide value in understanding the impact to industry stakeholders. Specifically, the MPIW will continue to map the previously discussed authentication protocols (e.g., SRC spec, 3DS 2.0, W3C, and FIDO) to identify key industry issues, benefits, and challenges. It plans to publish its findings in the first half of 2020.