FEDERAL RESERVE BANK OF BOSTON™

REPORT

Securing Mobile/Digital Payments in a Global, Transit, and Faster Environment

MPIW April 2018 Meeting — Summary of Key Findings
August 10, 2018

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

The Mobile Payments Industry Workgroup (MPIW)[1] is comprised of stakeholders focused on eliminating barriers to the successful adoption of mobile and digital retail payments in the U.S. The purpose of the April 2018 meeting was to discuss current industry developments related to: 1) EMVCo[2] specifications for secure remote commerce and 3-Domain Secure 2.0;[3] 2) transit open-loop mobile payments; 3) global digital wallet solutions; and 4) potential impacts of faster payments on mobile and digital payments.

I. Industry Developments to Secure E-Commerce Payments

There is growing concern that the lack of uniformity in remote commerce creates opportunity for bad actors and hinders the progress made by the payment ecosystem to reduce card-not-present (CNP)[4] fraud. In October 2017, EMVCo released *EMV Secure Remote Commerce Technical Framework* (SRC Framework).[5] The final specification is expected to be released in late 2018 or early 2019. From the perspective of the MPIW, it was important to understand how the SRC Framework will impact the e-commerce environment and how it relates to the implementation of the *EMV 3-D Secure Protocol and Core Functions Specification* (3DS 2.0).[6] Panelists[7] shared their perspectives on the SRC Framework and its objective to solve industry e-commerce challenges, as well as the U.S. implementation of 3DS 2.0 – how it will work, interoperability considerations, and prospects for merchant and issuer adoption.

EMVCo Secure Remote Commerce Framework

The SRC Framework defines a technical framework and specification that enables merchants to obtain a consistent, secure payload of customer payment information that can be used to facilitate payment authorization for remote commerce transactions through existing channels. The SRC Framework offers a streamlined payment experience that works across channels, browsers and devices, providing consumers

[1] The MPIW is convened by the Federal Reserve Banks of Boston and Atlanta. See http://www.bostonfed.org/bankinfo/payment-strategies/index.htm.
[2] EMVCo is a consortium that manages the security specifications for chip-based payment cards (EMV), including payments tokenization and the 3DS protocol. It is jointly owned by American Express, Discover, Visa, MasterCard, JCB, and Union Pay.
[3] 3-Domain Secure (3DS) is a secure communication protocol used to enable real-time cardholder authentication directly from the card issuer to improve online transaction security and support the growth of e-commerce payments.
[4] Card-not-present (CNP) is a payment made for a purchase using a payment card, where the cardholder/card is not physically present to allow the merchant to validate the cardholder at the time of purchase (e.g., by U.S. postal mail, telephone, or internet).
[5] EMVCo (2017, Oct.) *EMV Secure Remote Commerce Technical Framework Version 1.0*
[6] For more information on 3DS 2.0, see Pandy, S. (2017, Jan. 17). *Why 3-Domain Secure should be adopted in the U.S.* Retrieved from https://www.bostonfed.org/publications/payment-strategies/why-3-domain-secure-should-be-adopted-in-the-us.aspx.
[7] Representatives from Visa, Mastercard, RSA Security LLC, and Princeton Identity participated on this panel.

The authors would like to thank members of the MPIW and meeting participants for their engagement and contributions to this report.

with a consistent checkout and a common mark used by participating card networks and merchants. This SRC standard digital mark[8] will allow customers to recognize the payment cards accepted online, similar to the NFC[9] "waves" symbol on a POS terminal. Merchants can display the digital mark on their website checkout page independently, by integrating with each card network, or via a payment gateway.

The SRC Framework was not intended to redesign the merchant checkout experience but rather to make it more efficient by increasing sales conversions and reducing shopping cart abandonment; driving higher authorization rates; and reducing fraud in the ecosystem. Fraud vulnerabilities associated with e-commerce websites and mobile apps are minimized through secure transmission of payment and related checkout data; while decreasing repetitive manual primary account number (PAN) entries reduces shopping cart abandonment.

The greatest efficiency can be realized by resolving the authorization rate gap, particularly for CNP transactions. Because the SRC Framework is not a wallet, the card networks centrally store customer device and account information (i.e., PAN) to verify that the customer is associated with a particular mobile device or browser. When a transaction is initiated, the device or browser can recognize customers as they log in and authenticate to a merchant site using biometrics or passcodes (e.g., one-time password (OTP)) rather than a static password. This centralized approach will benefit issuers with greater visibility into potential payment risk or fraud events, payment authentication, and enhanced authorization.

In the long-term, EMVCo intends to include optional interoperability of the SRC Framework with tokenization, dynamic data, and domain restriction controls[10] for CNP transactions. Payment tokenization improves authorization approval and lifecycle management by enabling issuers to collect more data about the underlying token requestor (TR)[11] for a tokenized transaction (e.g., whether or not it is a merchant with strong fraud management tools). Many issuers have already reported higher authorization rates with EMV tokenized transactions. The SRC Framework will be interoperable with 3DS v2.0 as well, but merchants will decide whether they want to invoke 3DS for their customers.

MPIW members raised concerns about consumer awareness, merchant integration, and compatibility with other industry-related standards. Brand recognition already exists for the card networks' digital wallets, which supports their ability to build consumer awareness of the digital marks described in the SRC Framework. Discussions about merchant integration are ongoing as some stakeholders still require the customer to complete an online purchase "form-fill" screen, which can pose interoperability challenges

[8] The SRC Framework defines the SRC Mark as "a payment or checkout mark that identifies the SRC experience available to the consumer for a digital shopping application."

[9] 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. NFC-enabled mobile phones incorporate a smart chip (secure element) that allows the phone to store the payment app and consumer account information securely and use the information as a virtual payment card.

[10] The *EMV Payment Tokenisation Specification – Technical Framework Version 2.0* (2017) defines token domain restriction controls as "a set of parameters established as part of payment token issuance by the Token Service Provider that will allow for enforcing appropriate usage of the payment token in payment transactions." Examples include: use of the payment token with particular presentment modes (e.g., contactless, e-commerce); use of the payment token at a particular merchant that can be uniquely identified; and verification of the presence of a token cryptogram that is unique to each transaction.

[11] A token requestor (TR) is an entity that procures payment tokens from a TSP to use to complete a purchase (e.g., mobile wallet providers, shopping applications, web browsers, card issuers, merchants, acquirers, acquirer processors, and payment gateways). TRs must register and comply with a TSP's proprietary requirements and will receive a Token Requestor ID and need to implement the specified Token API. The TR can then request tokens from the TSP to provision to customer NFC-enabled mobile devices containing secure elements or other storage if HCE.

with different browsers and lead to transaction abandonment. The SRC Framework will support interoperability in the online channel and let consumers know exactly what to expect regardless of card network or merchant site.

There have been some discussions between EMVCo and the World Wide Web Consortium (W3C)[12] about how the SRC Framework will work with the WebAuthn specification for strong authentication being developed by the W3C and Fast Identity Online (FIDO) Alliance[13] (which focuses on authentication at the device level), but more clarity is needed.[14]

3DS 2.0 – Past, Present, and Prospects for U.S. Adoption

3-Domain Secure v1.0 (3DS 1.0) was created 15 years ago to accelerate the growth of e-commerce and reduce fraud by preventing unauthorized use of debit and credit cards.[15] The protocol's three domain structure includes the merchant/acquirer domain, issuer domain, and interoperability domain. 3DS 1.0 required issuers to authenticate all cardholders with a PIN or password entered into a pop-up screen during an online purchase. 3DS 1.0 had low adoption in the U.S. because it was browser-based, used static data elements, required consumer enrollment, and did not support mobile-initiated payments.[16] These issues resulted in high shopping cart abandonment for participating merchants and negatively impacted their ability to control the customer experience.

EMVCo released a more robust version of 3DS (v2.0) in October 2016. 3DS 2.0 provides global interoperability and a consistent consumer experience across mobile app and browser e-commerce channels and connected devices (e.g., Internet of Things (IoT)).[17] Risk-based authentication (RBA) is performed in the background, only prompting for step-up authentication (e.g., OTP, biometrics, and out-of-band) with higher risk transactions, significantly reducing customer friction. Furthermore, requesting static data from customers that could be easily compromised (e.g., passwords, pre-established question responses, card expiration date, etc.) are not permitted in the new protocol, replaced by the dynamic step-up challenges mentioned above. Many new data elements have been made available in the protocol to help issuers perform a better risk assessment. Effective RBA should result in a very small percentage of transactions needing step-up authentication, which reduces issuer operational costs (e.g., call centers) and increases transaction approvals.

Merchants decide if step-up authentication is needed for a higher risk transactions[18] and can invoke 3DS. When a merchant invokes 3DS during online checkout, the merchant may choose to share purchase information, device data, and other details (e.g., email address, mobile phone number, shipping, billing and IP addresses) with the issuer to authenticate the cardholder and confirm the purchase. The issuer can use

[12] The World Wide Web Consortium is an international community that develops open standards to ensure the long-term growth of the web. See http://www.w3.org/.
[13] The FIDO Alliance develops specifications and certifications to enable an interoperable ecosystem of hardware-, mobile-, and biometrics-based authenticators that can be used with many apps and websites. See https://fidoalliance.org.
[14] The Webauthn specification defines an API enabling the creation and use of strong, attested, scoped, public key-based credentials by web applications, for the purpose of strongly authenticating users. See https://www.w3.org/Webauthn/.
[15] Three global card networks have their own implementations of 3DS, Visa *Verified by Visa*, Mastercard *SecureCode*, and American Express *SafeKey*.
[16] Europe realized over 50 percent merchant adoption.
[17] 3DS 2.0 functions separately from v1.0, which will phase out as 3DS 2.0 matures.
[18] A transaction may be flagged as higher risk based on a company's risk-decisioning model, for example, when a customer's mobile device used to make a purchase does not match the previous mobile device used by that customer.

RBA to passively authenticate the cardholder or use step-up authentication based on the customer risk profile. Issuers maintain control of the authentication flow because they are liable for all 3DS-initiated transactions that they approve.

Financial institutions (FIs) and merchants asked if the 3DS 2.0 RBA approach would reduce false positives, stop fraud, and improve the consumer shopping experience. RSA Security LLC[19] has been using 3DS 1.0.2[20] in its fraud solutions for over 10 years in Europe and marginally in the U.S., and has supporting risk engine data to estimate the fraud detection rate that will be realized as the new protocol moves forward. RSA shared data from mid-2015 through early 2017 to show how the fraud prevention intelligence of its Access Control Service (ACS) risk engine has grown over time.

For example, the RSA risk engine captured 97 percent of fraud attempts by intervening[21] with only five percent of the customers. Of those five percent who were interrupted to stop potential fraud attempts in the first half of 2017, the fraud ratio was 2:1 (i.e., number of legitimate versus fraudulent transactions that were interrupted). While this number may seem high, the genuine-to-fraud ratio in the industry can range from 10:1 to 20:1, depending on the effectiveness of the risk engine. Interrupting a few good transactions to block 97 percent that are fraudulent is considered a good result and shows that the 3DS 2.0, if backed by a capable risk engine, can perform effectively as it is rolled out globally.

RSA also shared data on how the risk engine performance translates into savings for FIs and processors. FIs that use an effective risk-based 3DS ACS lose an average of 3.5 basis points ($35.00) for every $10,000 of genuine transactions that they approve. For many FIs, this represents a significant increase in revenue and increased operational benefits. Some of the larger European FIs that use this system report saving over $10 million per month on operational costs and chargebacks. Merchants see more genuine e-commerce orders and less fraud, which has a downstream benefit to all stakeholders.

RSA surveyed merchants to gauge plans for participation in 3DS 2.0 and found that 57 percent plan to adopt 3DS 2.0 when it is available. Similarly, a 2017 Javelin survey of 500 merchants showed that approximately 44 percent already used 3DS 1.0 and 19 percent plan to adopt some form of 3DS in the future.[22]

Currently, a few issuers and merchants have begun testing the 3DS 2.0 protocol with the card networks and ACS providers as part of the "early adopter" phase. This testing will continue through the remainder of the year, with general availability of 3DS 2.0 in early 2019. A successful rollout will require expansive industry education and programs to drive necessary stakeholder awareness and behavior.

[19] RSA Security LLC, formerly RSA Security, Inc., is a U.S. computer and network security company.
[20] 3DS 1.0.2 provides issuers with the option to utilize an RBA approach (as opposed to challenging every customer), allows for "pre-loading" the card Bank Identification Numbers (BINs) (eliminating customer enrollment), and can also remove the use of static data elements (e.g., passwords) in place of dynamic authentication such as SMS OTPs. However, this requires issuers to utilize an Access Control Server (ACS) provider who can offer that kind of solution, and not all issuers are aware of these providers or the benefits.
[21] In this context, "intervening" is when a customer is asked to further authenticate himself with an additional mechanism such as an SMS OTP, biometric test, mobile app query, or other method.
[22] Javelin Strategy & Research (2017, Sept). *Financial impact of fraud study*. Retrieved from https://s3.amazonaws.com/dive_static/paychek/Financial_Impact_of_Fraud_Study_FINAL.pdf.

Many European issuers are reviewing 3DS 2.0 protocol to determine if it will help them adhere to the recent Payment Services Directive 2 (PSD2)[23] regulation. The PSD2 regulation is discussed in more detail in Section III - Global Digital Wallet Solutions.

II. Transit Mobile Payments

Transit authorities in the U.S. continue to seek ways to improve the efficiency and lower the operating costs of public transportation. One area of focus has been to reduce the use of cash with electronic solutions, initially with closed-loop fare media, and now with account-based systems that support open-loop contactless card and mobile payments. The migration to EMV chip cards and NFC mobile solutions have made the transition to mobile payments easier.

Industry stakeholders have generally believed that expanding mobile payments to transit would help to support adoption of mobile payments for other use cases, particularly retail payments. With active implementations of contactless open payment systems underway at several transit authorities, it was a timely topic for the MPIW to discuss with stakeholders engaged in this business. The objective of the panel was to inform and engage the MPIW in a discussion about transit open payment systems, the challenges faced by U.S. transit agencies in managing multiple standards and maintaining interoperability within the current ecosystem, and how the transit mobile experience may help the adoption of retail mobile payments.

Several U.S. transit agencies are adopting new payment systems that support NFC-based mobile wallets and contactless cards, as well as mobile QR-code ticketing apps, all of which help to improve the customer transportation experience. Panelists included representatives from the Chicago Transit Authority (CTA), which implemented an open payment system in 2014; the Massachusetts Bay Transportation Authority (MBTA), planning to roll-out an open payment system by 2020; and American Express (AmEx), which has a transit mobile payment strategy that includes industry education, partnerships, and solutions.

Chicago Transit Authority (CTA)

In 2014, CTA launched a new contactless fare system, which supports the *Ventra* fare card[24] and contactless open payments. Today, 92 percent of its transactions are contactless (most are closed-loop Ventra cards and a very small number are open payments) and eight percent of transactions are paid with cash.

With 1.5 million rides each day, CTA is most concerned about service and customer access to the transit system. Mobile payments create an opportunity for a transit authority to standardize access across all modes, expand ridership, reduce fraud, and enhance user experience. In 2015, CTA launched the Ventra mobile app, which supports fare payment and travel information for Chicago's three regional transit agencies – CTA, Metra Rail, and Pace.

Contactless payments and mobile ticketing can decrease operator and customer costs, reduce fraud, and offer greater efficiencies for consumers. Open-loop payments replace some closed-loop cards and related expenses for transit agencies. A mobile ticket allows visual verification and helps prevent fare evasion. If

[23] 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. PSD2 requires financial institutions to grant third-party providers access to a customer's online account/payment services in a regulated and secure way.
[24] For more information, see https://www.ventrachicago.com/howitworks/.

the rider does not have a mobile app, the conductor can direct them to download the app to purchase a ticket. The mobile device also enables rider-tracking and fare-activation data through use of geolocation, which can support better service planning and identification of any suspicious activity. In the future, CTA would like to provision a virtual Ventra card to a mobile device (e.g., as part of a Pay wallet), which will require a mechanism to make the transit card the default payment method. This would create opportunities for advertising, loyalty, and trip and fare planning.

Massachusetts Bay Transportation Authority (MBTA)

The Massachusetts Bay Transportation Authority (MBTA) plans to launch an open payment fare system in 2020. The MBTA wants the new system to support all fare products to address customer price sensitivity and accommodate different types of riders.[25] The MBTA's goal is to build muscle memory to increase adoption of new payment methods. For occasional transit users, the MBTA seeks to provide a simple "zero user interface" experience, where riders can use their phones to tap the reader and walk through the fare gate without pre-purchasing any rides or passes. However, the process to handle account management and receipts is complicated and needs to be addressed.

The MBTA plans to become completely digital with standardized payment methods across different transit modes. For example, a new fare system for the commuter rail will replace paper tickets and receipts with a digital version. Depending on the location and mode of transit, the system may be gated or gateless, and customers will be able to tap in and out, multiple times per day. The MBTA will exclude QR codes from its digital plan because they are too time-consuming, require acceptance of a wide range of user devices, and negatively impact the ability to quickly process travelers. For transit authorities, mobile ticketing and payments rely on speed.

Challenges to Implementing New Transit Platforms

Public transit authorities must abide by Title VI of the Civil Rights Act of 1964.[26] To avoid any legal challenges, the transit agency's fare policy must demonstrate that it does not discriminate in its transportation systems and does not have a disproportionate impact to minorities and the underserved. The transit operator must accept all payment methods (e.g., cash, closed-looped fare media, open-loop contactless credit/debit cards, NFC mobile payments, etc.) to avoid excluding any customer segment from accessing service. Federal guidelines also require that a transit agency hold hearings and consider public comments on proposed changes to transit fares and services. This complex review process can sometimes delay timely introduction of new technology.

Making significant changes to a fare system must factor in time to implement, clear communication to transit riders, and adequate staff training. Fare pricing changes are particularly sensitive and must be implemented thoughtfully, as these changes can result in unintended consequences (e.g., customer

[25] The MBTA is committed to providing non-discriminatory service and ensuring that no person is excluded from participation in, denied the benefits of, or otherwise subjected to discrimination in MBTA's programs, services, or activities on the basis of race, color, or national origin, as protected by Title VI of the Civil Rights Act of 1964. The MBTA will continue to accept cash and closed-loop payments with its new fare system, in addition to accepting open-loop payments.

[26] Title VI (42 U.S.C. §2000d et seq.) was enacted as part of the landmark Civil Rights Act of 1964. It prohibits discrimination on the basis of race, color, and national origin in programs and activities receiving federal financial assistance. For more information, see https://www.justice.gov/crt/fcs/TitleVI-Overview. The Federal Transit Administration works to ensure nondiscriminatory transportation. See https://www.transit.dot.gov/title6.

confusion when shifting from one system to another). Some challenges associated with implementing transit open payment solutions include how to drive consumer use of NFC mobile payments, business impacts, as well as new security and risk considerations.

Card Network Support for Transit Open Payments

American Express (AmEx) and other card networks support transit authorities, issuers, acquirers, and system integrators; and participate in transit forums and industry association groups, such as the U.S. Payments Forum's Transit Contactless Open Payments Working Committee.[27] Interested stakeholders are working collaboratively to identify possible solutions that address the challenges associated with the implementation of contactless open payments within the unique U.S. public transit market.

The card networks work closely with relevant stakeholders to provide technical guidance for implementing contactless card and NFC mobile transit open payment use cases in the U.S. Because transit payments are low value/high volume and require extremely rapid throughput speed, transit agencies are considering new technology solutions to process open payment transactions. For example, to address such transit payment needs, AmEx has developed solutions that support delayed authorizations,[28] transaction aggregation, pre-authorizations, and other processes.

Some U.S. transit authorities are considering transaction aggregation in which multiple small dollar value transactions are aggregated (e.g., daily or weekly) before obtaining an authorization. Transaction aggregation can reduce costs and offer greater flexibility for transit agencies.[29] The card networks have established aggregation rules that enable transit agencies to offer daily and weekly capping, and charge each rider's payment card on a daily or weekly cycle once these caps have been applied.

Another option under consideration is pre-authorization for open payment transactions, in which a set dollar amount is reserved on the customer's credit/debit card when the final amount of the transaction is not known at the time of entry. However, pre-authorizations are unpopular, particularly with regular riders, and may adversely impact economically disadvantaged riders. Risk-based authentication may offer a better alternative.

Ultimately, educating riders and building awareness about the advantages of using contactless card and mobile for open-loop transit payments and to increase adoption is a responsibility of all the relevant stakeholders: transit agencies, issuers/acquirers, and card networks.

III. Global Digital Wallet Solutions

The objective of the third panel[30] was to inform the MPIW about similarities and differences between U.S. developed wallets and those from other countries, and how they could operate in the U.S. payments market.

---

[27] For more information, see http://www.uspaymentsforum.org/working-committees-sigs/transit-contactless-open-payments-working-committee/.
[28] A delayed authorization request is sent any time after a customer has been permitted entry to travel. U.S. Payments Forum (2017, Sept). *Technical solutions for transit contactless open payments use case 1: Pay as you go/card*. v1.0. Retrieved from http://www.uspaymentsforum.org/wp-content/uploads/2017/09/Transit-Use-Case-1-Technical-Solution-V1.0-FINAL-Sept-2017-2.pdf.
[29] Aggregation gives transit operators the flexibility to offer a range of other fare constructs such as free transfers and time-based tickets.
[30] Panelists represented MindBody, Stripe, and Financial Innovation Now.

Panelists discussed the expansion of global digital wallets such as China's Alipay[31] and WeChat Pay[32] into the U.S. market, as well as the growth of mobile wallet solutions in India (PayTM[33] and Tez[34]).

Minimal credit card use and the centralized nature of China's e-commerce market have facilitated the rapid expansion of mobile/digital payments in China. Alipay and WeChat Pay have grown significantly over the last five years to dominate the Chinese mobile/wallet payments environment.

In countries with very large populations and many under/unbanked consumers, (e.g., China and India), the use of QR codes in different use cases has helped to drive widespread adoption of mobile payments.[35] Unlike NFC Pay wallets (e.g., Apple Pay, Google Pay, and Samsung Pay), QR codes are device-agnostic and easier to implement and use. These wallets typically work with a two-party network. The mobile app may be connected to the consumer bank account, credit or debit card, or cash.

QR code payments only require the mobile phone to display or capture the QR code, creating less friction in the payment process. GrabTaxi Asia, a ride-sharing service similar to Uber, is an example of a frictionless mobile app. It also includes GrabPay, which enables consumers to make other types of purchases. Connecting different use cases seamlessly has made these solutions successful because the payment feature is complementary to other wallet features.

From a global perspective, Alipay and WeChat Pay want to support the Chinese tourist market in the U.S. Many Chinese travelers use their phones to pay and are less likely to use cash, or may prefer not to carry cash when traveling. Notably, nearly three million Chinese tourists travel to the U.S. each year,[36] which has driven Alipay to partner with First Data and Blackhawk to build acceptance of its wallet with U.S. POS and online merchants. Several other U.S. companies, including PayPal[37] and Green Dot, have formed relationships with Alibaba and/or Tencent to allow Chinese consumers to use Alipay and WeChat Pay with participating U.S. merchants.

Integrating Alipay or WeChat as a payment method with a U.S. merchant or other business can be done through an application programming interface (API). However, U.S. regulations may interfere with the process. For instance, non-profit entities (e.g., universities) cannot accept Alipay or WeChat payments because these transactions must be treated as donations. Some U.S. merchants that operate in countries such as China and India may be unlikely to accept these mobile wallets if they do not fit within the merchant's business model.

---

[31] Alipay was launched in 2006 and is owned by Ant Financial Services Group and Alibaba Group. According to ECNS, 82 percent of transactions made by its 520 million users were initiated via mobile in 2017. See Liping, G. (2018, Jan. 4). Mobile devices handle some 80% of Alipay's online payments in 2017. *ECNS.cn*. Retrieved from http://www.ecns.cn/business/2018/01-04/286997.shtml.

[32] In 2011, Tencent launched WeChat Pay, a payment app with a messaging function that reports over 900 million active monthly users. WeChat users scan their QR codes to pay for goods and services or to send messages to hail taxis or purchase real estate. Parker, E. (2017, Aug. 11) Can WeChat Thrive in the United States? *MIT Technology Review*. Retrieved from https://www.technologyreview.com/s/608578/can-wechat-thrive-in-the-united-states/.

[33] PayTM is India's largest mobile payments service.

[34] Google's Tez is an app that links to bank accounts via the Unified Payments Interface (UPI), which is a payment standard and system created by the National Payments Corporation of India, as a joint venture between Indian banks to enable technology to make payments between banks. Tez users can send and receive payments to each other without using bank account details or a phone number. This technology uses the Audio QR (AQR) ultrasound technique (similar to Bluetooth) to pair phones.

[35] For example, some Chinese shops and restaurants print out and display static barcodes that customers scan to pay from their mobile phone.

[36] U.S. Commerce Department (2017). *2.97 million Chinese nationals visited the U.S. in 2016, spending $33 billion dollars*.

[37] PayPal has a contract with Alibaba that enables Chinese to buy through American merchants, while U.S. consumers can use PayPal accounts to buy in China.

In India, mobile payments are largely supported by the launch of the Unified Payments Interface (UPI), which enables users to initiate payments and transfer money between bank accounts in real-time through any compatible mobile app. PayTM, Google Tez, and WhatsApp[38] recently adopted UPI and run on top of a bank account system comprised of approximately 50 FIs.

Walmart's global operations include China and India. Regardless of location, Walmart prioritizes its business strategy when considering the payment methods to accept. Accordingly, Walmart has decided not to accept Alipay, and does not believe that this decision has impacted sales.

Amazon offers payment solutions that enhance the customer purchase experience and increase global sales and accepts Alipay.

Global Authentication Approaches and Regulations

In India, strong customer verification is driven by the government's authentication and national identity policy. India's Aadhaar identification program issues a unique 12-digit identity number to residents of India based on biometric (fingerprint, iris scan) and demographic data. The Reserve Bank of India required all commercial banks, urban and state cooperative banks, payment banks, ATM operations, and authorized card payment networks to migrate to an Aadhaar-based biometric authentication method for electronic payment transactions by March of 2018. PayTM has already integrated fingerprint authentication into its e-wallet ecosystem and has launched an Aadhaar-based client-authentication system.

Similar to India, China favors a common authentication standard to be integrated with its central identity database and has a national ID system based on phone registration, requiring wallets to be authenticated and have set daily dollar limits. Both Alipay and WeChat have their own versions of authentication; WeChat uses a biometric protocol.

Attitudes and approaches toward authentication vary around the world. In the U.S., many companies are very customer-centric and opt for a frictionless customer experience over tighter security controls. Consumers in other countries expect friction and are willing to accept more rigorous authentication methods. For example, the U.S. migration to EMV chip cards did not require PIN (for debit and credit) because of concerns with customer friction as most U.S. consumers do not use PIN for credit card purchases. However, in the UK, if customers are not prompted to enter a PIN, they may question the transaction. In Europe, PSD2 mandates multi-factor authentication, which internet and technology companies believe will introduce additional friction into the ecosystem even though European consumers have become accustomed to extra security steps in the transaction process.

Future POS Environment

Panelists predicted that the current POS checkout environment will transition from deploying large, full-scale terminals to mobile devices, with portable checkout solutions and limited "cash only" aisles. Voice authentication and artificial intelligence will drive enhanced customer experience and authentication for

[38] WhatsApp is a mobile app that supports sending and receiving a variety of media: text, photos, videos, documents, and location, as well as voice calls.

payments. As the POS environment evolves, terminal providers will need to build capability for different wallet solutions. It will be at the merchant's discretion to decide which payment methods and/or devices to accept based on customer preferences. Mobile wallets will not have to converge, but a wallet integrator may be needed to seamlessly address multiple types of wallets.

It is difficult to envision a common global payment system. Typically, retail businesses, whether POS or online commerce, is viewed through the lens of the merchant. However, as commerce expands globally, technology companies are trying to determine how to make payment methods across countries less complex to support different ways of doing business. Participating in global commerce is particularly challenging for small merchants, which makes helping them achieve global reach an important consideration.

IV. Implications of Faster Payments[39] on the Mobile Payments Environment

The final panel[40] provided an update on the progress of faster payment developments in the U.S. and discussed two active implementations: The Clearing House (TCH) Real-Time Payment Solution (RTP) and Early Warning Services' (EWS) Zelle.[41]

TCH Real-Time Payments (RTP) System

The Clearing House launched RTP in collaboration with its 25 FI owners in November of 2017. RTP is a real-time payment system designed to address gaps in digital payment options and will enable consumers and businesses to securely send and receive immediate payments directly from their bank accounts. Developing a real-time payment system required coordination among FIs of all sizes and their service and technology providers.

Similar to wire transfers and ACH, RTP is expected to become part of the core industry infrastructure and underpin FI client-facing services with the potential to support many use cases including person-to-person (P2P) and business-to-business (B2B) payments, but it will not replace traditional payment networks. RTP is a 365/24/7 credit push network (no debits), with instant funds availability – the FI receives acknowledgement of acceptance or rejection of the transaction within seconds.

RTP supports the transfer of funds and Requests for Payment (RFP). RFP enables individuals and businesses to request money from other people or entities. RFP can be used to send an invoice to another company or for P2P and bill payments. Because the account-holding/issuing FI knows its customers best and owns the fraud liability, it provides the information to the receiving FI. Large billers support the RFP solution because the response message includes all the necessary data needed to process an RTP payment without any intervention.

RTP will clear and settle faster payment transactions in the background. Eventually, other faster payment vehicles like Zelle, Visa, and Mastercard could clear and settle transactions in real-time by sending a

[39] Faster payments, also known as real-time or instant payments can be sent or received 24/7, with real-time (e.g., minutes or hours) access to payment status information for senders and receivers and immediate availability of funds for receivers.
[40] Panelists represented BetterBuyDesign, The Clearing House, and Early Warning Services.
[41] Zelle is a U.S.-based digital payments network owned and operated by EWS. EWS is a bank-owned technology company that serves a diverse network of approximately 2,500 financial institutions, government entities, and payment companies. It is owned by Bank of America, BB&T, Capital One, JPMorgan Chase, PNC Bank, US Bank, and Wells Fargo.

message through RTP. Because FIs with mobile platforms can also clear mobile transactions using RTP, some are adopting a "mobile first" strategy.

RTP has robust security standards. Participating FIs will be required to use step-up authentication when needed and TCH has the right to audit or terminate an FI from the system at any time. TCH is also building an anti-fraud detection system on top of RTP. While TCH will not stop a transaction, it will identify such transactions for FIs to examine more closely.

Currently, RTP is focused on domestic payments, but in the future it could support cross-border real-time payments with other countries that have also moved to real-time payment systems.

RTP participation is challenged by lack of FI staff experience with faster payment systems, the lack of customer education about funds availability, and ecosystem issues. Many FIs have not created a new customer product since the launch of online banking 20 years ago. Since then, most new products have been incremental builds. RTP is new and FI product managers have little to no experience developing completely new FI products. They need to be trained on faster payments and new thinking on rules, risks, and processes before creating products for RTP. Another challenge is to ensure that customers (potential users of RTP) understand when funds are available through RTP and how it works differently than other payment networks.

Finally, there are several ecosystem issues. Most developed countries support the ISO 20022 Financial Services – Universal financial industry message scheme[42] and either have or plan to deploy a faster payment solution. Using ISO 20022, central banks will have consistent messaging to enable faster cross-border payments. However, many FIs are opening up development through APIs rather than through an ISO 20022 message. TCH did not develop APIs for RTP and currently, entities that connect to RTP must use ISO 20022. TCH is encouraging the development of APIs as a means for customers to connect to FIs to leverage RTP versus using ISO 20022. TCH is also supporting standardization where it makes sense and will be working with the industry on those efforts.

FIs that have begun to use RTP have realized efficiencies through automation and the elimination of batch processing, which has reduced the need to increase staff. RTP also reduces counterparty credit risk that stems from delays in receiving funds, and handles fewer exceptions than ACH or check systems.

Zelle

Zelle is a P2P payments mobile app created through a joint venture by the largest U.S. FIs. The service can support P2P payments using a standalone mobile payment app or through integration with participating mobile banking platforms. Consumers can enroll in Zelle through their FI's mobile banking app or directly in the Zelle mobile app using an email address or mobile phone number. Users can send money to recipients with a participating U.S. bank account using the recipient's email or mobile phone number. Zelle leverages the ACH network to transfer funds between consumer bank accounts. Currently transactions are processed within two to three days. In the future, Zelle could connect via RTP to clear transactions in real-time.

[42] ISO 20022 Financial Services – Universal financial industry message scheme is an ISO standard for electronic data interchange between financial institutions. For more information, see https://www.iso20022.org/about_iso20022.page.

EWS manages the risk-decisioning process on the backend for participating FIs. For example, data such as the device fingerprint, operating system (OS) version, and customer profile are used to generate a risk score for the FIs. Other backend checks can be performed with the mobile network operator to verify the sender's or recipient's mobile phone number. The governance model for Zelle also supports step-up authentication, in which the FI can decide whether or not to pass a transaction despite a recommendation by EWS to decline it.

Sending FIs that offer Zelle are responsible for educating customers about the associated fraud risks. FIs should examine their customers' payment behaviors and trends, identify patterns, and if necessary, prompt customers to re-confirm the receiving party before sending money. If funds are sent to an incorrect or fraudulent recipient, the customer is responsible for the loss, not the FI. In its terms of use, Zelle explains that customers use the service at their own risk and warns that customers must provide correct information. Regardless, not all customers fully understand that they are liable for funds transfers made to recipients because they provided inaccurate information (e.g., email, phone number).

V. Key Findings

1. The e-commerce environment is rapidly changing and expanding, making its security paramount. New security solutions and technical specifications seek to reduce fraud in the ecosystem and should be monitored as the industry evolves.

    a. The SRC Framework will be a new e-commerce specification for the industry that seeks to improve the e-commerce process by providing a consistent customer checkout experience to reduce shopping cart abandonment, increase authorization rates, and reduce fraud. As with any new changes to the payment system, stakeholders seek further understanding and clarification of its goals and potential impacts.

    b. Many stakeholders support the goal of 3DS 2.0 to help reduce fraud in the payments ecosystem, but without any live implementations yet, it offers minimal insights to help stakeholders prepare for adoption. The MPIW will continue to monitor 3DS 2.0 adoption and any challenges or impacts to the industry.

2. The transition that many transit authorities have made or are in the process of making towards implementing open-loop fare systems presents challenges, but offers many opportunities and benefits to transit agencies and customers. Increased mobile payment adoption among transit customers is likely to stimulate further adoption in other industry verticals.

    a. Legacy transit systems will remain for a while as new payment systems are implemented in some regions/transit authorities.
    b. The expansion of open-loop transit payment implementations in U.S. and Canadian transit systems will afford riders greater convenience and opportunity to regularly use contactless mobile payments without having to obtain closed-loop fare media.

3. Mobile and digital wallet adoption has grown in other countries, such as China and India, which promote mobile QR code models versus NFC. The industry should monitor developments with

these international wallets to understand how they support connectivity across multiple mobile applications abroad and the potential impacts in the U.S. as local businesses begin to accept these payment methods in some venues.

4. New digital and mobile use cases, such as faster and P2P payments are taking root in the U.S.; however, considerable stakeholder education is still required to gain broad acceptance from issuers, merchants, and consumers and address any new risks or challenges. These new use cases may provide the value-added benefits needed to accelerate mobile/digital growth.