Mobile Payments Industry Workgroup | April 18, 2019

Innovation across Mobile Payments: Alternative Checkout Models, Chinese Wallets, Fintechs, and Mobile Network Operators

MPIW December 2018 Meeting — Summary of Key Findings

Susan Pandy, Ph.D., and Marianne Crowe

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 December 2018 meeting was to discuss current industry developments related to: 1) mobile/digital payment adoption trends; 2) the impact of alternative checkout models on mobile payments; 3) the global expansion of Chinese mobile wallets; 4) fintech charter and alternative solutions; and 5) mobile network operator (MNO) developments for payment authentication.

I. U.S. Mobile/Digital Payment Adoption Trends

The meeting began with an overview and discussion of consumer mobile payment trends, based on a recent Javelin study.[2] Adoption has fallen short of expectations in the U.S., where less than 32 percent of consumers used a mobile device to pay in store between 2015 and 2017. Mobile wallet usage was below 20 percent (e.g., Samsung Pay – 10 percent, Google Pay – 12 percent, Apple Pay – 16 percent, and retailer wallets slightly higher at 18 percent). Although thirty-nine percent of consumers still do not see the value of using a mobile wallet in lieu of traditional payment methods, customizing retail wallets to offer rewards programs may attract more users.

A fragmented market with multiple payment options (e.g., swipe, dip, and tap) and an inconsistent checkout experience create consumer confusion and contribute to the lack of widespread adoption. The key to accelerating adoption is to develop solutions that prioritize the consumer experience and drive habitual use. Some stakeholders believe that near field communication (NFC)[3] contactless technology can build habituation to accelerate mobile payments growth.

Mobile person-to-person (P2P) payment solutions, such as Zelle[4] and Venmo,[5] simplify P2P payments between accounts at different banks or within non-bank solutions and increase mobile payment adoption. However, industry stakeholders need to provide broader education to consumers about the differences between mobile payments for

1 The Federal Reserve Banks of Boston and Atlanta convene the MPIW. See http://www.bostonfed.org/bankinfo/payment-strategies/index.htm.
2 Javelin (2018, Sept.). Mobile wallet wars: A battle for consumer loyalty. Available at https://www.javelinstrategy.com/.
3 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. Some 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.
4 Zelle is a U.S.-based digital payments network owned and operated by Early Warning Services, a bank-owned technology company that serves 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.
5 Venmo is a mobile payment service owned by PayPal. Venmo accountholders can transfer funds to others via a mobile phone app. Both the sender and receiver must reside in the U.S.

purchases and P2P transfers to other individuals or informal businesses, which are irrevocable.

Businesses beyond retail are considering how mobile can support evolving real time payment system use cases (e.g., faster payment of an insurance claim), but understand that faster payment solutions will need to address interoperability to succeed.[6]

Engaging younger generations in financial services is a challenge. Younger consumers may be digitally aware and technologically perceptive, but they lack a strong financial foundation. Financial service providers should develop customized approaches to reach this segment of the population. For example, a financial institution (FI) may target university students, whose needs may vary based on the location or type of school they attend (e.g., large state school v. regional). Financial institutions should survey this group to understand their financial goals and tailor services based on their preferences.

II. Alternative Checkout Models

Mobile technology drives much of the innovation at the point-of-sale (POS) checkout. To enhance the customer experience, merchants are implementing alternative checkout models, which include scan and go[7] features, self-checkout, no checkout, mobile NFC or QR code wallets, buy online pickup in store (BOPIS), and reserve online pickup in store (ROPIS), which allows customers to confirm that the items they want are in stock before paying for them. With so many payment options to choose from, merchants must evaluate which solutions to deploy, which solutions customers prefer, what factors influence omni-channel solutions, and which solutions spur further innovation. For example, merchants need to be aware that BOPIS is a card-not-present (CNP)[8] transaction, but ROPIS is card-present.

The first panel[9] shared their perspectives on the challenges and opportunities of leveraging technology to create unique experiences for their customers. They discussed how traditional checkout models are changing, including the benefits and pain points derived from alternative solutions. Panelists offered insights into how merchants think about checkout, alternative models available, and alternatives to simplify the payment process and enhance the customer experience.

---

6 For a discussion about The Clearing House Real-Time Payment solution, see Pandy, S. and Crowe, M. (2018, Aug.) Securing mobile/digital payments in a global, transit, and faster environment.
7 "Scan & go" allows customers to use the mobile device to scan items as they shop, pay via mobile phone, and skip the checkout line.
8 Card-not-present (CNP) indicates a purchase made with a debit, credit, or prepaid card where the cardholder/card is not physically present (e.g., payment made via phone, internet, or mail), so that the merchant cannot validate the cardholder at the time of purchase.
9 Panelists represented Amazon, Merchant Advisory Group, Nordstrom, Walmart, and P97 Networks, a startup company with the petroleum and convenience store industry to provide mobile commerce technology solutions that enhance fuel and in-store purchases with tools to help customers locate stores and use loyalty programs.

Nordstrom tested several alternative checkout experiences with mixed results. Using mPOS in its full-line stores was challenging. Large footprints and the need for clerks to wrap items or remove security tags adversely affected the intended convenience, which led Nordstrom to discontinue the service. However, their experience with BOPIS and ROPIS proved successful in getting customers into the physical store with an omni-channel solution.

Nordstrom also relaunched its loyalty program to leverage the customer's mobile phone number for identification in both the online and POS channels and provide a broader view of the customer. Because many customers do not carry their Nordstrom private label cards, Nordstrom permits customers to pay for in-store purchases without the physical card, using their card accounts[10] and a texting service. The Nordstrom customer sends a text to a designated number to "get my card" and receives a QR code used to access the customer's account credentials stored on file to process the payment.

Walmart prioritizes customer relationships over payments and continues to explore opportunities to leverage mobile payments to enhance that experience. The Walmart mobile app offers benefits beyond the "Walmart Pay" feature. Walmart understands that customers focus more on convenience than the omni-channel as part of their shopping experience. However, more customers are going digital, so the retailer must assess what that means to their business. Enabling the convenience of an omni-channel experience that allows customers to order/buy online and pickup in store is a major investment for a retailer with 4,000 locations and even more POS terminals. Walmart wants to design its physical stores to better map to the digital experience and minimize the need to retrain staff. Capturing and securely storing profiles in the cloud will help Walmart understand its customers' shopping behaviors and preferred payment methods.

The Sam's Club[11] model does not use NFC or QR codes and is open to registered members only. Because customers have a relationship with Sam's Club, they can scan their items and leave the store without physically checking out (the store has only one entrance and exit). This model provides a positive experience but may not work in stores where customers are not pre-registered.

Using technology to improve the checkout experience with order ahead and pickup in store is popular with many quick service restaurants. However, the technology requires user testing to address any problems that might affect the customer experience. For example, a customer orders food ahead, and upon arrival for pickup, cannot find parking and is unable to retrieve their order, but is still charged. This results in a financial loss to the customer and a negative experience because the business did not consider this scenario. Some restaurants use geolocation to confirm that a pre-order customer has retrieved their

10 Private label credit cards are cards branded for a specific retailer, independent dealer, or manufacturer.
11 Sam's Club is a division of Walmart.

purchase before processing the payment. These examples show how technology can deliver a positive experience that is not only about the payment.

For petroleum and convenience stores, the long-term goal is to allow a customer to pay without leaving the vehicle and to enable payments at multiple points of contact: in store, at the pump, and from the car, including connected cars. To create a cohesive customer experience, P97 works with multiple POS systems and payment networks, but faces challenges related to legacy equipment, the imbalance of technology across stakeholders, and fuel pump rules designed for card-present transactions. Given the number of dispensers in use, the investment required to upgrade POS and fuel dispensers for NFC does not support a strong business case for tap and pay, which is why many oil companies are investing in mobile solutions that do not require NFC. Standardization to support interoperability across industries might help to address the technology imbalance across stakeholders. P97 is evaluating new options to deliver offers to the mobile phone, use the same app to pay at the pump and in store, and co-locate gas stations with convenience or fast food stores to share loyalty programs that enhance the customer experience.

Amazon manages payments across discrete business units through apps for the phone, music, Amazon Fresh/Prime, and video. Each business provides unique customer shopping experiences (e.g., Amazon Go,[12] Amazon Prime) and addresses different needs. Amazon processes card-present and CNP payments and related loyalty in the cloud. The payments challenge is also an information challenge because of blended payment users (e.g., between family members). Each unit's goal is to simplify the payment process and analyze how to leverage data to enable customers to buy via different channels (online or mobile). Maintaining rich data on customer preferences also helps to manage risk. This data may not be available in real time, so Amazon may use other security tools, such as data gleaned from digital traces, to supplement card data.

Retailers face several key challenges to drive adoption of mobile payments. They must decide which wallets and technology platforms to implement and how to prioritize implementations. They must also understand what the "digital customer" means to their businesses and the long-term impacts of today's decisions and make sound judgments based on robust analysis. Finally, it is important that they learn more about the value of real time payments to retailers and customers; and how to manage potential new risks.

While retailers agree that there is no one-size-fits-all solution, they see how mobile technology can change the customer experience across channels. Retailers must understand their customer data to know which checkout models their customers prefer. Offering only one checkout model will not satisfy all customers. For example, new

12] In January 2018, Amazon opened Amazon Go, an automated and checkout-free grocery store in Seattle. Amazon Go relies on cameras and weight sensors to recognize what shoppers remove or put back on the shelves. There are no cash registers or checkout lines. After leaving the store, customers receive billing information through their credit/debit cards on file.

customers may have different preferences than established customers; some may prefer only to buy merchandise in the physical store. Developing a new payment experience may take a long time, depending on the technology platform, number of vendors involved, level of integration, and employee and customer testing. The ultimate goal among retailers is to achieve an experience where the customer does not have to think about the payment.

III. Alternative Checkout Models: Security and Risk Considerations

A second panel[13] discussed the security of alternative checkout models and considerations for managing the risk of implementing innovative options. Speakers shared insights on how to balance convenience and frictionless checkout methods with the need for strong and continuous customer authentication. Alternative checkout models may integrate both card-present and CNP channels to improve the consumer experience (e.g., Uber, Lyft). However, stakeholders must still ensure that the seamless customer experience across channels is secure.

Consumer enrollment is the weakest link in securing mobile wallets. Merchants decide which approaches they want to use for strong customer authentication to deliver the best experience for the consumer. Some stakeholders suggest allowing customers to select their preferred authentication method. Out-of-band authentication is effective, and because enrollment is a one-time occurrence, customers may be willing to accept some friction. However, once merchants know their customers (through history, behavior, etc.), they should be able to process transactions without interruption.

3-Domain Secure 2.0 (3DS 2.0)[14] has addressed many of the limitations of the first specification. It provides global interoperability and a consistent customer experience, whether paying through a mobile app, mobile browser, other e-commerce channel, or connected device (e.g., Internet of Things). To reduce customer friction, risk-based authentication occurs in the background, only prompting for step-up authentication (e.g., one-time passwords (OTP), biometrics, and out-of-band) with high-risk transactions. Merchants can decide what additional information they share with FIs for step-up authentication. Some merchants indicate that the card networks are not consistent in their 3DS implementations and may offer or limit certain features.

---

13 Panelists represented Mastercard, SHAZAM, Synchrony, and Worldpay. Mastercard is a technology company in the global payments industry that performs payment processing that connects consumers, financial institutions, merchants, governments, and businesses in more than 210 countries and territories. SHAZAM is a debit network and processor for small and mid-sized financial institutions and merchants. Synchrony offers private label cards and co-branded financing for retailers. Worldpay is engaged in global commerce for card acquiring and digital wallets and helps merchants integrate digital wallets onto their websites.

14 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.

Using a third party provider to obtain customer information from MNOs through a customer's mobile phone is another authentication option. Digital IDs can match customers to their mobile devices and bind the device to the customer for card-on-file (CoF) systems. Panelists noted that before consumers can pay using their identity instead of a physical card, stakeholders must address the need to secure the identity.

EMVCo's[15] Secure Remote Commerce specification (SRC spec)[16] can support alternative checkout models in the online environment. The SRC spec describes how merchants can facilitate payment authorization for remote commerce transactions. It supports a streamlined payment experience that works across channels, browsers, and devices and provides consumers with a consistent checkout process and a common mark used by participating card networks and merchants. The secure transmission of payment and related checkout data minimizes fraud associated with e-commerce websites and mobile apps. Decreasing repetitive manual entry of card credentials reduces shopping cart abandonment. Some stakeholders recognize the benefits of streamlining payment options on a website and want to include private label cards. Others expressed uncertainty, noting the SRC spec's complexity (e.g., too many stakeholder roles), minimal requirements, and no commercial implementations.

Alternative checkout models are vulnerable to data breach and account takeover fraud (ATO).[17] This underscores the need to keep cardholder data out of the retailer's environment and away from the webpages and other services. As mobile payments continue to grow and account for a larger share of multi-channel transactions, retailers need to assess the customer's expectation for immediacy and balance that with strong fraud and security controls.

IV. Expansion and Acceptance of Global Wallets in the U.S.

This panel[18] explored opportunities and challenges for Chinese businesses and FIs that are expanding into the U.S. payments industry through partnerships with processors and

---

15 EMVCo is a consortium that manages the security specifications for chip-based payment cards (EMV), including payments tokenization and the 3DS protocol. American Express, Discover, Visa, MasterCard, JCB, and Union Pay jointly own EMVCo.

16 EMVCo (2018, Dec.) *EMV Secure Remote Commerce: Protocol and Core Functions Specification. Version 2.2.0.* For a discussion of the SRC Framework, see Pandy S. and Crowe, M. (2018, Aug.). *Securing mobile/digital payments in a global, transit, and faster environment*.

17 An account takeover attack (ATO) occurs when fraudsters use stolen consumer login credentials to access online accounts with merchants and payment service providers, use stolen personally identifiable information (PII) to change account settings, and take over the account to make purchases. ATO can occur at merchant sites (i.e., breaking into accounts on the merchant's website to pass as a returning customer), at online payment service sites (i.e., breaking into accounts of online payment services, such as PayPal, Apple Pay, Amazon Payments), and through online banking.

18 Panelists represented Ant Financial, BetterBuyDesign, Union Pay, and First Data Corporation.

merchants. Chinese consumers, including tourists, students, and ex-patriots, spend an estimated $30 billion with U.S. merchants every year.[19] Most of that volume is spent using the traditional card model on UnionPay,[20] Visa, Mastercard, and American Express cards issued in China. Chinese consumers spend millions of dollars with U.S. merchants, paying with Chinese QR code-based wallets Alipay[21] and WeChat Pay.[22]

Ant Financial, the financial arm of Alibaba and the company behind Alipay, started its U.S. operation five years ago. At the end of the third quarter of 2018, the Alipay mobile wallet had 700 million active users in China and 1 billion users globally together with its joint venture partners. Alipay is a digital wallet and "lifestyle super app" through which users conduct a broad range of activities (e.g., make appointments, buy food, reserve taxis or hotel rooms, etc.). Ant Financial's goal is for Alipay to deliver the same seamless experience to Chinese tourists in the U.S. that they offer in China. Alipay also partners with large technology companies (e.g., Apple, Google, Amazon, Uber, Airbnb) to make those services available within and outside of China. Ant Financial facilitates cross-border payments in 40 countries and invests in digital wallets outside of China, including Paytm[23] in India and Kakao Pay[24] in Korea.

Alipay is a QR code-based mobile wallet. The QR code is dynamic, changing every minute to reduce the possibility of being re-used. Most of Alipay's QR codes are user-presented, but the authentication process varies by market. A sophisticated artificial intelligence-driven risk engine identifies users, their behaviors, device location, and other factors in order to detect low- versus high-risk transactions. The risk level determines whether users have to perform step-up authentication by entering a personal identification number (PIN) or six-digit passcode assigned during the enrollment process. Newer versions of Alipay leverage facial recognition to compare a user's facial features to their national ID.

---

19 U.S. Commerce Department (2017). 2.97 million Chinese nationals visited the U.S. in 2016, spending $33 billion dollars.
20 UnionPay is a payment card network headquartered in Shanghai, China. As a major card scheme in mainland China, it provides transaction processing services and offers UnionPay branded payment products. UnionPay offers traditional cards and a mobile wallet, which it is modifying to enable Chinese consumers to make purchases in the U.S. UnionPay branded cards are accepted in 174 countries and regions around the world.
21 Alipay 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 percent of Alipay's online payments in 2017. ECNS.cn. Retrieved from http://www.ecns.cn/business/2018/01-04/286997.shtml.
22 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/.
23 Paytm is India's largest mobile payments service.
24 Kakao Pay is the financial technology division of Kakao and allows POS payments, P2P transactions, bill pay, web banking, etc.

The Chinese market is more conducive to accepting QR codes for mobile payments. QR codes tend to dominate in markets where merchants need a mobile phone infrastructure, but have limited resources to support NFC POS upgrades. In China, QR codes require minimal investment for payment acceptance. They provide opportunity for the large number of mom-and-pop shops to print merchant-presented static QR codes that consumers scan to enable merchants to accept mobile payments. For added security, China limits the purchase dollar amount to approximately $50 for merchant QR code payments.

UnionPay is the largest card issuer in China. It has issued over 7 billion cards cumulatively in 52 countries and regions with their logo, half of which are contactless. UnionPay switches card transactions between its issuing and acquiring members and implements payment network rules. Besides traditional payment cards, UnionPay also enables mobile payments for its customers, regardless of the underlying technology. Because legacy technology infrastructure (e.g., chip, contactless, QR code) may differ between geographic regions, the UnionPay mobile app gives customers the capability to use the technology that is prevalent in the local market (e.g., scan, tap or pay in-app).

All payment methods comply with EMV specifications for contactless chip and PIN, and QR code. Whether the transaction is card-present or CNP, the rules and rates are the same, and the liability resides with the issuer. Most transactions are chip and PIN or authenticated using 3DS version 1.0 and take only one second to process. In China, consumers tend to use the UnionPay cards and wallet for everyday and occasional high-end purchases and Alipay and WeChat Pay more for common daily purchases.

U.S. citizens who travel to China can obtain a U.S.-issued UnionPay branded credit card or prepaid card, which they can use at Chinese merchants, but they cannot use the Alipay or WeChat wallet in China, unless they open an account at a bank in China to fund the mobile wallet.

First Data Corporation (FDC) integrates global wallets (e.g., Alipay and WeChat Pay) with U.S. merchants and other companies. According to FDC, the average transaction value for a Chinese customer is approximately 25-40 percent higher than what the major card networks report for any merchant, making the acceptance rate of these wallets very attractive to retailers. Merchants who advertise their acceptance of the Union Pay mobile wallet tend to see a 2-10 percent increase in usage on their e-commerce websites.

V. Evaluating the Need for a Fintech Charter and Alternative Solutions

This panel[25] included a startup financial services company, a virtual FI that works with fintechs, and a legal expert. They explored the advantages and disadvantages of the

25 Panelists represented an independent consultant, Alston & Bird, LLP, Radius Bank (a full-service virtual bank), and Payzer, which offers a mobile financial tool that features a mobile app and online payment application to accept payments in the field and enable credit for customers with instant on the spot approvals.

special purpose charter and application process, as well as alternatives to fintech charters, such as collaboration with FIs or sandbox approaches.

With a natural tension between innovation and regulation, fintechs have an expectation that regulators will help them achieve compliance. In recent years, more fintech companies have engaged with the U.S. Office of the Comptroller of the Currency (OCC)[26] and requested changes to laws requiring money transmitter licenses[27] from all 50 states. The OCC issued its responsible innovation framework to support direct engagement for businesses and published a whitepaper in 2016 that created the Office of Innovation to consider special purpose charters for fintechs.[28] This initiative allows companies to apply for national bank charters without accepting deposits, which the OCC asserts is permitted under the 1864 National Bank Act.[29] Therefore, the OCC is open to charters for companies that solely offer payment solutions.[30] The OCC finalized the licensing procedure to obtain a charter in July 2018 and recently reported that as many as 40 potential applicants had expressed interest in the charter.

Before applying for a special purpose fintech charter, a company should assess how the charter would fit into its long-term corporate strategy and affect the ability to control its own future. The charter significantly reduces, and potentially eliminates, the need for businesses engaged in money movement or lending to obtain money transmitter licenses in every state, which is otherwise a lengthy and costly process.

As an alternative to the charter, fintechs can seek partnerships with FIs. Financial institutions can help fintechs facilitate discussions with regulators and solve business problems. The breadth of industry understanding and knowledge of regulations can be daunting to a startup, and an FI's ability to engage with regulators is an important facet of a partnership. Radius works with fintechs that prefer an alternative to a charter and faster time to market. Radius can help the business deliver solutions within a specific timeframe, raise funding, and become operational by overcoming hurdles and eliminating

---

26 The OCC is an independent bureau of the U.S. Department of the Treasury that charters, regulates, and supervises all national banks and federal savings associations as well as federal branches and agencies of foreign banks.
27 A money transmitter or money transfer service is a business entity that provides money transfer services or payment instruments. U.S. money transmitters are part of a larger group of entities called money service businesses (MSBs). Under federal law, 18 USC §1960, businesses are required to register for a money transmitter license in each state where their activity falls within the state definition of a money transmitter.
28 U.S. Department of Treasury. Office of the Comptroller of the Currency (2016, Dec.). Exploring special purpose national bank charters for Fintech companies.
29 The National Bank Act of 1863 was the first attempt to establish a central bank after the failures of the First and Second Banks of the U.S., and it served as the predecessor to the Federal Reserve Act of 1913. The act allowed the creation of national banks, set out a plan for establishing a national currency backed by government securities held by other banks, and gave the federal government the ability to sell war bonds and securities.
30 The New York Department of Financial Services and the Conference of State Bank Supervisors filed a lawsuit against the OCC claiming that it could not issue such charters, but these cases were dismissed. However new lawsuits were submitted and remain open.

inefficiencies in the solutions. Many fintechs consistently try to eliminate pain points for customers who seek simplicity, but it can be difficult to keep up with customer expectations. Fintechs have to learn how to prioritize changes and address only the most critical problems, which is another area where a more experienced partner can provide guidance.

Radius advises fintechs on how to be proactive with regulators, and educates them on the regulatory perspective and the need for particular financial regulations. Conversely, Radius helps regulators better understand the needs of the startup businesses. Fintech companies, such as Payzer, seek thoughtful partners like Radius, to help them engage with regulators, and to interpret and comply with applicable laws. Ultimately, the FI/fintech effort is a partnership.

VI. Mobile Network Operators and Authentication Developments

Mobile network operators can play a pivotal role in the identity and authentication ecosystem. Increased consumer engagement with connected services through their mobile devices has created potential business opportunities for MNOs, which provide devices, connectivity, content, and other personalized digital services. Trusted digital authentication is the foundation for delivery and consumption of these services.

A representative from Nok Nok Labs[31] led a discussion on current MNO developments influencing the mobile payments industry, particularly those for authentication and identity management. Key initiatives include Mobile Connect, GSMA's Rich Communication Services (RCS), Project Verify, and Fast Identity Online Alliance (FIDO).[32]

Mobile Connect

Mobile Connect is a cooperative effort among MNOs to normalize identity and authentication as a service. Adoption is currently underway in different regions of the globe to offer a service that allows customers to log in to websites and apps from any device, without usernames or passwords. Instead, customers are identified using their mobile phone number. Customers create an account via a Mobile Connect logo on a website, mobile app, or through their MNO to use the service. Once registered, customers can select the Mobile Connect logo whenever it appears as a login option. They receive a mobile phone message that may require additional verification, such as a personal code or PIN. Mobile Connect verifies the customer and completes the login process.

---

31 Nok Nok Labs develops next generation authentication for cloud, mobile and Internet of Things (IOT), deployed through MNOs, fintech, banking, healthcare, and IoT customers. They also work with FIDO and W3C on relevant standards.
32 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.

GSMA's Rich Communication Services (RCS)

Rich Communication Services (RCS) is a GSMA communication protocol between MNOs, and between the MNO and the mobile phone. RCS replaces SMS messages with a richer text-message system. GSMA created the protocol in 2007, but mobile carrier participation and other factors delayed progress. MNOs are currently evaluating whether to combine RCS and identity capabilities. In 2018, Google began working with global MNOs to adopt the RCS protocol and developed its own protocol, "Chat," based on the RCS Universal Profile that will eventually supersede SMS. At this time, implementation by MNOs and mobile operating systems is limited.

Project Verify

Project Verify is a new authentication initiative that Tier 1 U.S. MNOs (AT&T, Sprint, T-Mobile, and Verizon) developed.[33] It offers customers a streamlined method to verify their identity when creating a new account on a website, and to replace passwords and OTPs for logging in to existing accounts at participating sites with secure, device-based multifactor authentication and biometrics.

Through Project Verify, MNOs provide capability for issuers to authenticate the customers and their mobile devices by accessing their risk signals and account information. These authentication risk scores consider the valid phone number, approximate real-time location of the customer, how long they have been customers and have used the device (account tenure), type of phone account, biometrics and information about components inside the customer's phone that are only accessible to the MNOs (e.g., cryptographic signatures tied to the device's SIM card), and IP address.

Stakeholders (e.g., issuers, merchants) must integrate Project Verify into their systems to enable adoption. The solution app is intended to be bundled on all mobile devices (i.e., pre-loaded into software on the phone) and requires customer registration. Websites could allow the Project Verify mobile app (and the user's MNO) to pre-authenticate the user and then interactively log the user in without a username and password. MNOs also anticipate a feature to allow customers to pre-populate data fields on a website (e.g., name, address, credit card number, etc.). Project Verify will be able to select the types of data to share between the customer's wireless provider and a website on a per-site basis, or share certain data elements across sites that leverage the app for authentication and e-commerce.

A key consideration for the use of MNO-sourced data in risk scoring/mitigation solutions is the availability of consistent MNO-signal based information from all MNOs within a

33 The Project Verify legal entity is a joint venture owned in equal equity participation of the four U.S. Tier 1 MNOs.

given geography. The Project Verify initiative in the U.S. seeks to address this issue through a cooperative effort to normalize and aggregate MNO-based risk scoring from a single source. Consequently, recent efforts to terminate access to MNO-sourced data available through aggregators may be disruptive.

Fast Identity Online Alliance (FIDO)

FIDO compliant strong customer authentication (SCA) solutions have been deployed in mobile apps in Japan and China for many years. Some companies (e.g., Cigna, Intuit, and T-Mobile) have recently deployed FIDO compliant mobile app solutions in the U.S. With the support of Microsoft, Google, and Mozilla, relying parties[34] (including issuers and merchants) can now add browser-based FIDO SCA solutions on any device that supports a Chrome, Edge, or Firefox browser, as well as the previous mobile app-based solutions. The new browser-based FIDO capabilities include FIDO2, the World Wide Web Consortium (W3C)[35] Web Authentication specification (WebAuthn), and the Client-to-Authenticator Protocol (CTAP).

All versions of the FIDO protocols (e.g., universal authentication framework, universal second factor, and WebAuthn) use public key cryptography techniques to provide strong, multifactor authentication. During registration with an online service, the user's client device initiates the creation of a new key pair. It retains the private key on the device and the public key resides with the online service. The client device performs authentication when it signs a challenge to prove possession of the private key. The client's private keys must be unlocked locally on the device by the user. The local unlock is accomplished by a user-friendly and secure action, such as swiping a finger, entering a PIN, speaking into a microphone, inserting a second-factor device, or pressing a button.

FIDO, W3C, and EMVCo are coordinating their authentication efforts. FIDO is now an official International Telecommunication Union (ITU) and International Standards Organization (ISO) standard. EMVCo's 3DS 2.0 protocol has defined a data field to share FIDO data to facilitate the liability shift and EMVCo is currently working to define the details of the FIDO data to be provided.

VII. Findings

1. Role of mobile in alternative checkout models

More retailers are using mobile technology to leverage customer data to enhance the customer experience and reduce fraud. Retailers will implement the solutions that best

34 A relying party is a computer term used to refer to a server providing access to a secure software application. An application demonstrating the concept of relying party is software running on mobile devices, which can be used not only for granting user access to software applications, but also for secure building access, without the user having to enter their credentials each time

35 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/.

meet their customers' needs. Innovation at checkout will be a differentiator and NFC/contactless will be more widely accepted across merchants and influence incremental growth in consumer mobile payment adoption.

2. Securing the mobile checkout

Securing the online channel begins with customer enrollment, which should leverage multiple methods and channels for authentication. Businesses are testing the use of digital identity tools to strengthen customer authentication. In 2019, several new/enhanced tools will be available for implementation and assessment (e.g., digital and CoF tokenization, 3DS 2.0, SRC, FIDO authentication, and W3C). The industry may see a significant decline in the use of usernames and passwords in 2019, but a decrease in CNP fraud remains uncertain.

3. Rich customer data is critical to combat fraud and enhance customer experience

Retailers are trying to ensure a smooth and frictionless customer experience, and protect customer information. Effectively analyzing available real time customer data will become a critical tool in retailers' ability to balance fraud mitigation and customer experience.

4. Factors that impact decisions to innovate

Merchants must consider several factors (e.g., operational costs, fraud mitigation, handling returns, customer impacts, etc.) when developing their strategies to implement alternative checkout methods. This decision-making process will vary based on the type and size of the merchant and the channels in which it operates. No single approach applies to all types of merchants or customers.

5. Acceptance of global wallets for tourists to the U.S.

New partnerships between U.S. and Chinese businesses to enable mobile payment acceptance will expand significantly. As more U.S. merchants begin to accept AliPay, WeChat Pay, UnionPay, and others, it is important to monitor and assess impacts to U.S. FIs and merchants, as well as overall mobile payment adoption and growth in the U.S.

6. Growing role of fintechs

The payments industry may see the first company to receive a fintech charter in 2019. Stakeholders should monitor the process to understand the role these companies will play in the industry and the progress among FIs and fintechs that collaborate to coordinate with regulators and deliver innovative solutions.

7. MNO authentication services

Mobile network operators are becoming more active in efforts to secure mobile payments by leveraging their technologies to offer authentication and identity management

services. They will need to work closely with payment stakeholders to build awareness and adoption of their tools.

8. Standards

Both proprietary and open standards factor into the 2019 outlook for the payments industry. We have already noted several proprietary efforts, but the Accredited Standards Committee (ASC) X9[36] has undertaken the X9.134 initiative to develop a domestic mobile financial services (MFS) standard modeled after the *ISO 12812: Core Banking – Mobile Financial Services* standard and technical specifications published in 2017.[37] Standardization is essential for sound development of MFS features to allow: 1) interoperability between the different MFS components and functions; 2) ease of consumer experience and choice among mobile devices or products;[38] and 3) a secure environment to ensure trust in the mobile financial service provider (MFSP)[39] and enable FIs to manage risks. A national MFS standard in the U.S. can address some of the market fragmentation, create safeguards to address potential fraud, and drive greater adoption of mobile banking and payment services.

36 For more information, see https://x9.org.
37 ISO 12812 is a five-part standard that includes: Part 1 – general framework, adopted as an international standard, and Parts 2-5 adopted as technical specifications. Part 2 addresses security requirements, Part 3 mobile financial application management, Part 4 payments to persons, and Part 5 payments to businesses. The X9 work proposals for Parts 1 and 2 are available on the X9 Members website. ISO 12812 ultimately decided to include banking functions and app requirements within the overall language, rather than develop a separate part. X9.134 will include an evaluation of the use of mobile devices to enable a bank customer to initiate specific banking functions. For more information, see https://www.iso.org/news/2016/05/Ref2083.html and https://www.iso.org/standard/59844.html.
38 Including the ability to transfer MFSs from one device to another (i.e., portability).
39 The term "mobile financial service provider" (MFSP) is used in this standard to designate an institution that has created an MFS offering accessed by its customers via a mobile device. For example, Apple, Google, Samsung, PayPal, financial institutions, and other third-party mobile wallet providers are MFSPs. An institution that is part of an MFS value chain but does not provide a service via a mobile device is not an MFSP.