Mobile Payments Industry Workgroup | May 1, 2020

Mobile / Digital Payment Industry Trends in Distributed Ledger Technology, Cryptocurrency, Mobile P2P Payments, Fraud, and Authentication

MPIW January 2020 Meeting — Summary of Key Findings

Susan Pandy, Ph.D. and Marianne Crowe

The Mobile Payments Industry Workgroup (MPIW)[1] is composed of stakeholders focused on eliminating barriers to the successful adoption of mobile and digital retail payments in the U.S. The purpose of the January 2020 meeting was to discuss payment developments related to: 1) U.S. federal and state government initiatives that support distributed ledger technology (DLT) and digital assets; 2) developments in cryptocurrency and stablecoins; 3) the role of mobile person-to-person (P2P) payments[2] in driving faster payment adoption; 4) mobile payment fraud solutions; 5) authentication protocol implementations; and 6) current mobile/digital payment adoption trends.

The views expressed in this paper are those of the authors 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.
Thank you to the MPIW meeting speakers that provided comments and clarification to the content in this report.

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] Mobile P2P payments allow consumers to transfer funds from their account to another individual's account via a mobile phone. .

I. U.S. Distributed Ledger Technology, Blockchain, and Cryptocurrency Trends

Cryptocurrencies and their underlying blockchain technology have the potential to fundamentally impact the financial sector.[3] Blockchain, as a form of DLT, offers many potential benefits to financial institutions (FIs) including lower costs, improved transparency, and operational auditability. More specifically, blockchain creates a shared ledger that can reduce the duplication of information that occurs across FIs and intermediaries when they maintain their own databases and ledgers.

New technology startups are building services and businesses with blockchain, similar to how technology disruptors Amazon, Google, Facebook and Uber built software platforms and successful businesses through the connectivity provided by internet standards. However, blockchain developments remain nascent as these new businesses contend with U.S. regulatory challenges and becoming more secure and trustworthy systems.

The success of cryptocurrencies and blockchain technology is contingent upon how trustworthy these solutions become, beyond the basic security of the distributed ledgers. Law, regulation, and governance support trustworthy systems that can lead to broad adoption. Providers need to address legitimate government concerns and build confidence in new blockchain systems through transparency about how the processes work, what the benefits are, and develop straightforward solutions that secure adoption.[4]

A distributed ledger is a decentralized digital system (i.e., distributed across several computers or nodes) that operates a set of synchronized ledgers that are shared by multiple entities (i.e., no central authority or data store). DLT records the transaction of assets and their details in multiple places simultaneously. Unlike traditional databases, distributed ledgers do not require a central data store or administration functionality.[5] Instead, multiple nodes are responsible for updating the ledger or transactions if any data changes occur, and every node receives its own copy of the ledger.[6]

Blockchain is a type of distributed ledger system where various transactions (i.e., not only monetary) between parties are recorded redundantly and securely in multiple databases. A blockchain organizes data or records into blocks linked with each other and encrypted, using strict security protocols that require computational trust.[7] A block contains details such as the transaction timestamp and a link to the previous block, making it impossible to alter information about the records retrospectively. Unlike traditional databases, a blockchain allows only adding new data; existing data cannot be altered or deleted. Blockchains are useful for financial transactions because they help to reduce operational inefficiencies

[3] Not all cryptocurrencies use a blockchain (e.g., IOTA).
[4] *How Blockchain will impact the financial sector*. Retrieved from https://knowledge.wharton.upenn.edu/article/blockchain-will-impact-financial-sector/.
[5] DLT could reduce the traditional reliance on a central ledger used in financial markets and managed by a trusted entity, which could change how assets are stored or maintained, obligations discharged, contracts enforced, and risks managed.
[6] Every time a new transaction is added, it is encrypted and all the copies of the ledger are updated before being added to the ledger.
[7] In information security, computational trust is the generation of trusted authorities or user trust through cryptography. In centralized systems, security is typically based on the authenticated identity of external parties.

(leading to cost savings), provide greater security based on a decentralized system, and are immutable. Examples include Hyperledger,[8] Ethereum,[9] Quorum,[10] and R3.[11]

Cryptocurrency is a digital currency that serves as a unit of account or store of value. Traditionally, it did not meet the standard for a medium of exchange because of price volatility and lack of inherent value. The recent advent of stablecoins, which peg a cryptocurrency against a stable asset (e.g., fiat currency), has helped address some of these issues. Cryptocurrency uses cryptographical functions to conduct financial transactions (i.e., use of private and public keys directly between two parties). These transfers can be done with minimal processing fees and leverage blockchain technology to gain decentralization, transparency, and immutability.

U.S. Federal and State Government DLT and Digital Asset Initiatives

The first panel[12] discussed DLT, blockchain, and cryptocurrency trends in the U.S. at the federal and state levels. Paul Thanos, U.S. Department of Commerce (DoC), reviewed the role of technology in changing international trade and efforts to adopt DLT. Chris Rothfuss and Tyler Lindholm, co-chairs of the Wyoming Blockchain Task Force (the "Task Force"), explained the State of Wyoming's governance model for blockchain and cryptocurrency business development and how it was an opportunity for its technology sector.

U.S. Department of Commerce – Office of Finance and Insurance Industries (OFII)

Within the DoC, the OFII focuses on blockchain technology to understand its impact on innovation, U.S. economic competitiveness, and international trade.[13] Now that companies are at the adoption stage of blockchain and DLT, one of OFII's objectives is to identify a series of trade and business use cases including trade finance, governance, insurance, and supply chain management. The Office develops programs and policies to highlight the business impact of blockchain and DLT solutions, identifies impediments to its adoption, and, when appropriate, delineates U.S. trade policy priorities that can facilitate blockchain solutions. OFII is also closely tracking how various foreign governments are pursuing national blockchain strategies.

DoC is also supporting DLT initiatives that use blockchain to expedite engagement by small/medium U.S. businesses (SMBs) in international trade through collaboration with industry on private sector solutions that expand access to trade finance. DoC also organizes meeting between U.S. businesses and foreign governments to develop business opportunities (e.g., attending the Singapore FinTech festival).

---

[8] Hyperledger is an open source collaboration to advance cross-industry blockchain technologies. See https://www.hyperledger.org.
[9] Ethereum is a global, open-source platform for decentralized applications. See https://ethereum.org/.
[10] Quorum is an open source blockchain platform that combines the public Ethereum community with enhancements to support enterprise needs. See https://www.goquorum.com/.
[11] R3 is an enterprise blockchain software firm that works across multiple industries private and public to develop blockchain applications on Corda, an open-source blockchain platform. See https://www.r3.com/.
[12] Scott Moeller, CEO, mShift; Paul Thanos, Director, Office of Finance and Insurance Industries, U.S. Department of Commerce; Chris Rothfuss, Senate Minority Leader, Wyoming State Legislature; Tyler Lindholm, Representative, Wyoming State Legislature.
[13] The Office of Financial and Insurance Industries (OFII) works to enhance the domestic and international competitiveness of key U.S. financial services industries, focusing on policy, promotion, and analysis to expand U.S. financial services exports, attract investment to the U.S., and facilitate the growth and development of new and inclusive segments of finance.

OFII is involved in several activities focused on DLT and blockchain including strategic partnerships with Georgetown's Center for Financial Markets and blockchain businesses ConsenSys[14] and BurstIQ[15] and public outreach to provide information about blockchain to the marketplace. OFII is currently exploring collaboration with a financial regulatory agency to develop a toolkit that explains blockchain, its applicability to U.S. businesses, and its importance in a global context. The toolkit will help companies understand how to leverage DLT solutions for innovation.

The DoC does not have a regulatory role nor promote the use of cryptocurrency, but seeks to understand its adoption and commercial application globally and any relevance to U.S. competitiveness. According to Mr. Thanos, less than 1 percent of U.S. FIs use cryptocurrency as an asset, which the Securities and Exchange Commission (SEC) permits under the "qualified custodianship rule."[16]

State of Wyoming – Legal Framework for Digital Assets and Blockchain

The State of Wyoming is effective because it listens to the industry. Legislators Rothfuss and Lindholm recognized Wyoming government could play a greater role in digital assets, blockchain, and cryptocurrencies. Through their legislative efforts, Wyoming has been innovative and supported and promoted a legal framework for these new systems. Wyoming's Blockchain Task Force has offered a global forum to stakeholders seeking a rational governance model that includes definitions and a legal framework to reduce uncertainty and risk in the marketplace. It has also provided consumer protection and market fairness rules for digital assets.

Wyoming has passed 13 blockchain and crypto-related legislative bills to create the state's legal framework, and several other laws were passed in the 2020 legislative session. Changes include reclassifying digital assets as property under the Wyoming Uniform Commercial Code (UCC) and establishing special-purpose depository institutions (SPDIs) to support businesses that cannot secure traditional banking access, such as those within blockchain industries.[17] Fully-reserved fiat banks[18] can apply to be designated as an SPDI, which allows them to become custodians for crypto-assets.[19]

---

[14] ConsenSys is building Ethereum blockchain infrastructure and applications for new economic systems that are more open, efficient, and secure. See https://consensys.net.

[15] BurstIQ is a blockchain enablement company, offering enterprise-level blockchain solutions for the health and healthcare industry. See https://www.burstiq.com

[16] The SEC adopted amendments to conform the custody rule under the Investment Advisers Act of 1940 to modern custodial practices and require advisers that have custody of client funds or securities to maintain those assets with broker-dealers, banks, or other qualified custodians. See https://www.sec.gov/rules/final/ia-2176.htm. Some U.S. FIs that work with crypto-assets include Ally, Goldman Sachs, USAA, and Simple Bank.

[17] These Special Purpose Depository Institutions (SPDIs) will be required to have 100 percent reserves, cannot lend, will be for business depositors only, and will not be required to have FDIC insurance. The Wyoming Division of Banking will be the primary regulator.

[18] Fiat currency is legal tender whose value is backed by the government that issued it. The U.S. dollar is fiat money.

[19] A 2016 Board of Governors report on DLT discussed the need for a new kind of FI to integrate digital assets into the financial system to provide services around the storage, recordkeeping, and transfer of more-traditional financial assets, but not other traditional banking functions such as household and business lending. Mills, D., et. al. (2016). *Distributed ledger technology in payments, clearing, and settlement.* Finance and Economics Discussion Series 2016-095. Washington: Board of Governors of the Federal Reserve System. Retrieved from https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf.

According to the legislators, several new "blockchain banks" could bring over $20 billion in assets to Wyoming by the summer of 2020 and contribute an estimated $4 million in tax revenues.[20] Avanti Bank and Trust will be the first applicant to receive the SPDI charter and is expected to open in 2021.[21]

While the panel did not discuss blockchain or DLT in the context of traditional mobile/digital payments, there is relevance for future MPIW discussions. Blockchain could add a layer of security and trust to mobile and digital wallets and mobile P2P transactions because of its ability to carry a ledger of encrypted data with details of prior transactions. Every individual in the blockchain-enabled transaction would have a record of relevant transactions in the system, making it possible to transfer money with an inherent trust factor, with added protection that the transaction cannot be altered, and is available for everyone to review.

II. Cryptocurrency, Stablecoins, and Central Bank Digital Currency

Cryptocurrencies are disruptive and prone to price volatility, making some merchants reluctant to adopt them. In comparison, stablecoins can potentially serve as the backbone of financial applications on the blockchain. A stablecoin is a cryptocurrency that pegs its market value to a stable reference, such as the U.S. dollar, or the price of a commodity, such as gold. To achieve global acceptance, it would have to be private, decentralized, price stable, and scalable.

Stablecoins also face legislative, compliance, and licensing challenges. Some legislative efforts have sought to define stablecoins as securities, although since not all stablecoins are securities, other stakeholders believe they should be commodities. Classifying stablecoins as regulated securities might create consequences for the crypto industry. For example, stablecoin companies might have to register their offerings and comply with regulatory requirements. A company that facilitates stablecoin transactions might have to register as a broker-dealer. Other challenges include compliance with Know Your Customer (KYC)[22] and money transmission laws.

The second panel[23] discussed how cryptocurrency and stablecoins operate in the current market and their potential impact to the payment system. Panelists described four types of stablecoins: 1) Facebook's Libra digital currency, based on a basket of international currencies;[24] 2) those backed by another cryptocurrency (i.e., Dai token);[25] 3) fiat-backed;[26] and 4) U.S. Dollar Coin (USDC).[27]

---

[20] Wilcox, M. (2019, Sept. 16). Five 'blockchain banks' may open soon in Wyoming, *Wyoming Business Report.* Retrieved from https://www.wyomingbusinessreport.com/industry_news/banking_and_finance/five-blockchain-banks-may-open-soon-in-wyoming/article_e648eb5a-d8d0-11e9-ba85-7fb8deffe216.html.

[21] Martinez, A. (2020, Feb. 25). Thanks to Wyoming, The US will soon have a crypto bank. *CryptoBriefing.* Retrieved from https://cryptobriefing.com/thanks-wyoming-us-will-soon-have-crypto-bank/.

[22] Know Your Customer (KYC) is the process of a business verifying the identity of its clients and assessing their suitability, along with the potential risks of illegal intentions towards the business. KYC also refers to bank and anti-money laundering regulations.

[23] Panelists included representatives from CoinBase; BitPay; Bakkt; and Accenture.

[24] Libra is a blockchain digital currency proposed by Facebook. The currency and network do not yet exist; launch is planned for 2020. Libra stablecoins are backed by a "basket" of low-volatility assets, such as bank deposits and short-term government securities in currencies from stable and reputable central banks. See https://libra.org/en-US/.

[25] Dai is a decentralized stablecoin created by MakerDAO. One Dai equals one U.S. dollar and remains so until the token is removed from circulation. See https://cryptonews.com/coins/dai/.

[26] Fiat stablecoins are tokens associated with the value of a particular fiat currency (e.g., U.S. dollar), and hold their value fixed at a 1:1 ratio.

[27] See https://www.coinbase.com/usdc.

Libra's stability is backed by the inclusion of multiple international currencies, determined by its board of directors.[28] Stablecoins backed by another cryptocurrency (e.g., Dai token) face challenges from securities laws and high price volatility (e.g., Ethereum-backed[29] stablecoins may not be stable). Stablecoins backed by fiat currency are not backed by sovereign obligations (e.g., Tether).[30] The USDC is tied to the U.S. dollar and attached to a sovereign obligation (e.g., Coinbase).

US Dollar Coin Stablecoin

The US Dollar Coin (USDC) stablecoin is a virtual currency token that resides on the Ethereum blockchain and represents a claim on the U.S. dollar held in a U.S.-insured depository institution. Developed by an open architecture consortium, USDC stablecoins are instantaneous, price stable, and operate as a medium of exchange. These stablecoins are backed by U.S. sovereign obligations (e.g., only FDIC bank deposits and treasuries) and can be used for global remittances, international trade finance, and the equivalent of a U.S. savings account (e.g., theoretically, a consumer could hold USDC stablecoins in an FDIC-insured bank account that earns interest).

Sending money to another country through wire transfers or other regular remittance methods can be costly, amounting to approximately 7 percent in foreign exchange and/or remittance fees.[31] Using blockchain and stablecoins for global remittances presents a major market opportunity because the transaction cost can be reduced to less than 1 percent, (i.e., the cost to send one USDC unit is the same as sending 1000 USDC units), creates less friction and can be faster, according to the USDC representative.

Bakkt – Futures Market for Crypto Assets and Stablecoins

Bakkt helps consumers and institutional investors trade and spend digital assets and stablecoins.

Bakkt aggregates consumers' digital assets, enabling instant liquidity and empowering consumers to trade, transfer, and pay. Bakkt's focus on payments and consumer adoption includes development of a mobile app to perform these functions, paying with rebates, rewards, miles, and points.[32] To grow adoption, Bakkt enrolled merchants – including Starbucks – to accept Bakkt Cash as a payment method.

Bakkt's consumer mobile app does not accept deposits or withdrawals. The consumer receives a ledger entry on cryptocurrency that is already stored on the Bakkt registry. Citi supports Bakkt and manages its funds and consumer accounts. Bakkt affiliate companies, the New York Stock Exchange (NYSE) and Intercontinental Exchange (ICE), offer the security infrastructure for Bakkt to provide digital asset custody services to consumers.

Bakkt also launched a futures market for institutional investors and bankers to take delivery of Bitcoin. Both the Commodity Futures Trading Commission (CFTC)[33] and the New York Department of Financial Services regulate this market.

---

[28] The board of directors resembles the functions of a central bank and decides the "true" value of a currency.
[29] See https://ethereum.org/.
[30] According to Tether's website, as of Jan. 1, 2018, no issuance or redeeming services will be available to U.S. individual and corporate customers. See https://tether.to/.
[31] The World Bank (2019, Dec.) *Remittance prices worldwide.* Issue 32**.** Retrieved from https://remittanceprices.worldbank.org/sites/default/files/rpw_report_december_2019.pdf.
[32] Mobile app not yet launched.
[33] The Commodity Futures Trading Commission promotes the integrity, resilience, and vibrancy of the U.S. derivatives markets through sound regulation. See https://www.cftc.gov/

Bakkt participants undergo AML/KYC reviews, consistent with the CFTC-regulated markets, and connect via the ICE infrastructure. Bakkt's focus on compliance spans all aspects of its operations, including routine financial and security audits, and regulatory compliance reviews.

Accenture's Digital Dollar Project

The Digital Dollar Project (the "Project") is a partnership between Accenture and the Digital Dollar Foundation to advance exploration of a U.S. central bank digital currency (CBDC).[34] A digital dollar would be a government-sanctioned blockchain protocol, created and maintained by an independent, non-governmental group but administered by FIs and other payment organizations. In theory, cash brought into the system would be exchanged for digital U.S. dollars on a blockchain, with the cash held in special escrow accounts maintained by the Federal Reserve.

The Project encourages research and public discussion on the potential advantages of a digital dollar, convenes private-sector thought leaders, and proposes possible models to support the public sector. The Project plans to develop a framework for the practical steps necessary to establish a CBDC. In this way, the Project seeks to catalyze a digital, tokenized U.S. currency that would coexist with other Federal Reserve liabilities and serve as a settlement medium that offers lower cost, speed, and a more inclusive global financial system.

Central Bank Digital Currency

While the process of sending money has been slow to change, the demand for currencies with added functionality to support faster, more certain, accessible, and complex payments has accelerated and central banks are paying attention. Facebook's Libra and the rise of other digital currencies has induced central banks to investigate launching their own versions. A January 2020 report by the Bank for International Settlements indicated that more than 50 central banks were working on token-based digital money with a focus on general public usage.[35]

More than two-thirds of central banks have been investigating new payment applications, with many emerging as potential innovators to offer new possibilities to represent and transfer value.[36] For example, Sweden's central bank, Riksbank, was the first to pilot the deployment of a digital currency (e-krona). China plans to introduce a CBDC and the European Central Bank is exploring digital currency features. Uruguay is also running a pilot project for e-peso. A centralized electronic currency would require customers to open accounts at their respective central banks, rather than using a commercial bank, requiring central banks to monitor activity and prevent illegal activities for consumer-based accounts, thus creating more overhead for central banks.

Central banks are not the only organizations exploring ways to capitalize on the demand for new currency functionalities. The Facebook-supported Libra proposal highlights that private, non-state stablecoins may play an important role as a borderless payment medium. Similarly, other initiatives, including digital coins

---

[34] See https://www.digitaldollarproject.org/.
[35] Bank for International Settlements. (2020, Jan.) *Impending arrival – a sequel to the survey on central bank digital currency*. BIS Papers, No. 107. Monetary and Economic Department. Retrieved from https://www.bis.org/publ/bppdf/bispap107.pdf.
[36] *Ibid*.

from Goldman Sachs, JP Morgan, MUFG, and Walmart, seek to offer new payment technology and functionality that existing national currencies currently do not provide.

III. Role of Mobile P2P Payments in Driving Faster Payment Adoption

Faster payments are poised to reshape the payments industry by offering an array of alternatives to traditional payments. Some industry consultants estimate that mobile P2P payments will comprise the largest segment of faster payments and represent the strongest driver.[37] eMarketer projects that over half of mobile phone users (52 percent) will have made at least one P2P payment within the past month by the end of 2022.[38] Millennials (born 1981-1996) are the largest segment of mobile P2P users today, but other consumer segments are also sending money to friends and family as use of mobile apps, (e.g., Venmo, Zelle, Square Cash, Apple Pay Cash) increases.[39] The third panel[40] discussed the current state of U.S. mobile P2P payments, challenges and opportunities, and trends that will affect future strategic business decisions.

Financial Institution-Based Zelle

Early mobile P2P solutions were closed-loop services offered by non-bank third-party providers. Zelle emerged as the first FI consortium-driven P2P solution, providing a common FI brand and user experience that enabled consumers to conveniently move money between payer and payee at different FIs. As of January 2020, over 766 FIs and credit unions had signed up for Zelle and 378 FIs were live.[41]

In 2019, consumers sent 743 million transactions, valued at $187 billion, through the Zelle network.[42] The average spend was $245 per transaction, with consumers using the app at least three times per month. User demographics represented 14 percent boomers (born 1943-1960), 29 percent Gen X (born 1960-1980), 10 percent Gen Z (born 1993-mid-2000s), and 45 percent millennials.

A key requirement for adoption of mobile P2P is that the consumer enrollment process must be easy. Zelle's enrollment only requires an email and a phone number. Mobile P2P apps can also benefit from leveraging the phone's camera for a photo ID or using its address book. Older solutions required the consumer to submit their FI routing and transit number or for users to have accounts at the same FI. P2P apps that require manual entry of personal information and account numbers, or are restricted to proprietary mobile operating systems (OS), (e.g., Apple Cash), may be at a disadvantage.

User Experience and Education

While funds transfer and other features are important, the user experience must be a priority for any mobile P2P solution – it must be easy and frictionless. Consumer education is key because once funds are sent,

---

[37] Mercator Advisory Group (2019, Oct. 22). *Analyst Roundtable: Faster Payments 2019*. [Webinar]. Mercator estimates that P2P will constitute 32 percent of faster payment transaction volume by channel. Available at https://www.mercatoradvisorygroup.com/Webinars/Analyst_Roundtable__Faster_Payments_2019/.
[38] eMarketer. (2018, Dec.) *Who's using P2P payments in the US?* The Mobile Series [Infographic]. Retrieved from https://www.emarketer.com/content/the-mobile-series-mobile-peer-to-peer-payments-infographic.
[39] Early Warning Services (2018, April). *Early Warning Digital Payments Tracker*. Retrieved from https://www.earlywarning.com/press-release/zeller-study-finds-growing-use-digital-payments-across-generations.
[40] Panelists included representatives from Bank of America, Fiserv, and PTap Advisory, LLC.
[41] Zelle (2020, Jan.28). *Gift giving helps Zelle wrap up 2019 with double digit growth*. [Press release]. Retrieved from https://www.zellepay.com/press-releases/gift-giving-helps-zelle-wrap-2019-double-digit-growth.
[42] *Ibid.*

they cannot be automatically recalled from the receiver's account if sent in error (versus fraudulently). Consumers must ensure that they are sending funds to the correct email or phone number of the intended receiver. Zelle may occasionally prompt a sender to verify that they want to send the money before completing the transaction. In some instances, Zelle may use out-of-band authentication for extra verification, although the added friction is not preferred.

Non-Bank Mobile P2P Providers

According to one panelist, non-bank mobile P2P providers are not subject to the same costs and regulatory compliance as FIs that move money between demand deposit accounts (DDAs). Fintechs are creating good user experiences and some are reaching into offering solutions for consumer checking accounts, although it is too soon to know what adoption will look like.[43] Large technology companies (e.g., Facebook, Google, and Apple) that seek to offer consumer traditional banking products face challenges from regulatory approvals and possible lack of consumer trust.

Understanding Real-Time Payments

Consumers now believe that anything can be delivered, which is known as the "Amazon effect." This has raised consumer expectations for faster money movement, creating the need for FIs and fintechs to address this across multiple use cases. In the near-term, panelists see the most relevant use cases for faster payments to be payroll and emergency payments. For real-time payment (RTP) adoption to grow, businesses will need to update their systems to process RTPs. However, many companies still rely on ACH or legacy (i.e., batch-based) systems.

The Clearing House (TCH) launched a commercially-available RTP system in November of 2017.[44] Fiserv also offers real-time account-to-account transfers with plans to roll out bill payment in the near future.[45] Zelle, a consumer P2P service between FIs operated by Early Warning Services, plans to roll out a separate P2P service for small businesses.

Because not all mobile P2P transactions reach the recipient's account in real time, customers can be confused. The timing of deposits depends on the solution provider. Most P2P payments today still rely on the ACH Network, which is not a "real-time" network, but a batch system in which payments can take between 1-3 days to reach an account. Zelle uses the RTP system to provide real-time processing if the recipients are both enrolled in Zelle with participating FIs. Consumers lack an understanding of what is meant by "real-time," because they are accustomed to the instantaneous nature of card payments. However, the industry is educating consumers and small businesses about RTP.

---

[43] Cowley, S. and Tara Siegal Bernard. (2019, Nov. 13). Google makes a bid for banking, where tech firms go to stumble. *New York Times.* Retrieved from https://www.nytimes.com/2019/11/13/business/google-banking-checking-account.html.

[44] The Clearing House Payments Company L.L.C. owns and operates core payments system infrastructure in the U.S. and has launched a real-time payment system. TCH is the only private-sector ACH and wire operator in the U.S., clearing and settling nearly $2 trillion in U.S. dollar payments each day, representing half of all commercial ACH and wire volume. See https://www.theclearinghouse.org.

[45] Fiserv (n.d.). *TransferNow: The next generation of account-to-account transfers*. Retrieved from https://www.fiserv.com/en/solutions/customer-and-channel-management/online-banking-solutions/transfernow.html.

IV. Current Mobile Payments Fraud Landscape and Solutions

Constant data breaches continue to impede growth in consumer use of mobile devices and solutions to make digital payments. A changing fraud landscape has made it more efficient and scalable for a fraudster to penetrate a large database (e.g., Equifax) and not only obtain a vast amount of data, but also primary account numbers (PANs). While many authentication and security mechanisms help to make mobile payments more secure, card-not-present (CNP)[46] fraud costs the industry billions each year and mobile payments fraud is growing.[47]

The fourth panel[48] discussed mobile and online payment fraud trends, as well as the tools used to combat fraud. While the market is prophesizing the potential for artificial intelligence and machine learning to help address the CNP fraud problem, there is still a strong need and desire for access to more data to enhance risk decisioning and customer treatment (e.g., data that can help identify known, low-risk customers). Stakeholders want to know where to invest for fraud prevention and mitigation while remaining competitive.

More Data Collection and Sharing

The most important way for stakeholders to prevent fraud is more access to data. EMVCo's[49] 3DS[50] includes access to more data to assess transaction risk and to determine whether step-up authentication is needed for suspected fraudulent transactions. Regardless of the additional data afforded by using EMV 3DS, stakeholders should collect more data from other available sources to help prevent and mitigate fraud. Using more data to make a better risk decision will help to enhance the consumer experience.

Stakeholders may benefit from data received during the consumer enrollment process that is normally obtained during the KYC process. Issuers could potentially use enrollment data throughout the entire customer lifecycle, along with real-time data updates. The holy grail of fraud prevention is to ensure robust authentication and identity verification during the onboarding and origination phase that FIs can leverage throughout the customer lifecycle.

Balancing Low Fraud and Consumer Experience

Merchants want to strike a balance between maintaining low fraud rates and providing a seamless and positive customer experience. In some instances, a merchant may approve a potentially risky transaction to maintain a low fraud rate and because they may have more data about the customer. Using step-up authentication for higher-risk transactions introduces friction to the customer experience. Merchants want to minimize friction to avoid customer abandonment at checkout, which is why more data can improve the ability to approve more legitimate transactions without interruption and only create friction with additional authentication on a small percentage of transactions deemed high-risk. Many U.S. payment industry

---

[46] Card-not-present payment occurs when a cardholder/card is not physically present when making a purchase, preventing the merchant from validating the cardholder as the card owner.

[47] Sift (2020, March). *Digital trust & safety index: A rapidly-changing fraud landscape*. Retrieved from https://pages.sift.com/rs/526-PCC-974/images/digital-trust-and-safety-index-changing-landscape.pdf.

[48] Panelists included RSA Security, SHAZAM, Synchrony Financial, and TSYS.

[49] 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, secure remote commerce, and 3DS. American Express, Discover, Visa, MasterCard, JCB, and Union Pay jointly own EMVCo.

[50] EMV'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. 3DS 2.0 functions separately from v1.0, which will phase out as 3DS 2.0 matures.

stakeholders are developing strategies to deploy stronger authentication in response to the European Union's Payment Services Directive 2 (PSD2) requirement for strong customer authentication (SCA), which mandates the use of two-factor authentication for online transactions with some exceptions (e.g., merchant-initiated recurring transactions).[51]

Some merchants and issuers are working together to identify suspected fraud and stop the fulfillment process before goods are shipped. Establishing effective pre-authorization parameters for transactions is also helpful, and an area where EMV 3DS can help.

Use of One-Time Passwords (OTPs)

Panelists discussed whether one-time passwords (OTPs) offer sufficient customer authentication to prevent fraud for card-on-file (CoF)[52] and CNP transactions. One-time passwords are vulnerable to social engineering that convinces consumers to provide the OTP to supposedly trusted entities, such as through phishing attacks or when fraudsters impersonate a customer service representative from the consumer's FI.

An alternative solution would create a uniform method for retrieving mobile numbers and expanding the use of the mobile app. For example, many consumers only interact with their FI through their mobile banking app and are likely using a biometric to authenticate themselves. The app may be a better destination for sending the OTP. The problem with OTPs is that they have become a universal panacea, despite considerable innovation around facial, fingerprint, or behavioral biometrics. While OTP is a convenient solution, it is becoming less secure and requires the industry to assess improvements.

V. Authentication and Security Protocol Implementations

Three organizations involved in the development of secure payment systems (EMVCo, World Wide Web Consortium (W3C),[53] and Fast Identity Online (FIDO) Alliance[54]) have released authentication protocols to enhance the security of online and point-of-sale (POS) transaction environments. Panelists[55] discussed their perspectives on EMVCo's Secure Remote Commerce Specification v1.0 (SRC),[56] 3DS and card-on-file (CoF) tokenization,[57] as well as W3C's payment APIs, and FIDO's Client-to-Authenticator Protocol (CTAP). The different authentication protocols may have some overlap, so merchants and other stakeholders need to understand and analyze them for suitability with their business models. Broad adoption generally occurs over time, as these products need to be tested and fine-tuned. Other

---

[51] 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. SCA requires 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.

[52] Card-on-file is the process of collecting and storing payment credentials for future use in the remote commerce ecosystem.

[53] World Wide Web Consortium (W3C) is an international community that develops Web standards. See http://www.w3.org/.

[54] FIDO Alliance is an open industry association that develops authentication standards to reduce reliance on passwords. See https://fidoalliance.org.

[55] Panelists included representatives from Airbnb, American Express, Mastercard, and Netflix.

[56] EMVCo (2019, June). *EMV Secure Remote Commerce Specification v1.0.* This specification describes how merchants can facilitate payment authorization for remote commerce transactions across channels, browsers, and devices with 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.

[57] With card-on-file EMV payment tokenization, the merchant only stores payment tokens in their database rather than the actual PAN. This delivers various security benefits to the digital commerce ecosystem by reducing the risk and mitigating the impact of malware, phishing attacks, and data breaches.

considerations include the consumer experience, the level of friction introduced to the transaction, and the problems that merchants are trying to solve (e.g., shopping cart abandonment, customer fraud).

Netflix

It is critical to secure the CNP payments environment with fraud as a moving and growing target. One example is the card networks' initiative to create a new use case to tokenize CoF PANs for merchants.[58] Netflix recognized CoF tokenization as an opportunity to eliminate friction on recurring transactions and was an early adopter. According to the Netflix representative, CoF tokenization has had a significant positive impact on transaction approval rates and a reduction in chargebacks.

Netflix's business model is based on a $12 per month recurring subscription, creating a high volume of monthly transactions. While EMVCo's SRC is an attractive option to streamline acceptance of all of the digital payment wallets (e.g., Masterpass, Visa Checkout), Netflix views it as more suitable for merchant guest checkout models, not its subscription model. SRC eliminates the need for consumers to enter the full PAN and other relevant data for each merchant, which reduces the risk of transactions fraud by streamlining the online checkout process. Netflix will continue to evaluate the benefits that SRC can provide to its business model and customers.

Netflix's concerns related to 3DS and W3C focus on customer friction. 3DS 1.0 is still used in some countries where Netflix does business (e.g., India), which requires businesses to perform 3DS for every transaction, which slows down commerce. EMV 3DS (2.0) is risk-based, but still lacks broad issuer adoption in the U.S. Netflix tested W3C's Payment Request API and saw a negative impact to customer enrollment because it created friction by requiring the customer to enter a card verification value (CVV), but they are working as a member of W3C to help improve the process.[59]

Airbnb

In order to maintain a marketplace built on trust among individuals, Airbnb requires customer authentication and identity verification before a guest can complete a booking. Travel planning is a high commitment vertical where customers are willing to tolerate some friction while completing a booking and will typically complete the transaction, despite some friction in the process. Despite that behavior, Airbnb will always view customer friction as one of its largest business considerations because of its impacts on checkout conversion rates and repeat usage.

Airbnb operates in over 190 global markets and uses 3DS 1.0 in many markets, but it is in the process of integrating and testing EMV 3DS in advance of global market mandates for implementation. Based on their experience with 3DS 1.0, step-up authentication can result in a 50 percent chance that the customer will abandon the transaction. Anything in the form-fill process that is unusual or out of the ordinary for consumers (e.g., additional information beyond name, billing address, PAN) will also decrease conversion. This underscores the need for a fluid and consistent checkout experience that includes strong identity authentication while limiting impacts to conversion.

---

[58] In 2014, the introduction of technical specifications for end-to-end *payment tokenization* transformed the ability to secure mobile and digital transactions throughout the payment transaction flow with the release of the EMV Payment Tokenisation Specification – Technical Framework Version 1.0 (EMV v.1.0).[58] EMVCo published an updated version EMV Payment Tokenisation Specification — Technical Framework Version 2.0 (EMV v2.0)[58] in 2017. For more information on the evolution of payment tokenization, see Pandy and Crowe (2019). *Industry Perspectives on the Evolution of EMV Payment Tokenization*.

[59] A card verification value (CVV) is a 3-digit number on a Visa, Mastercard, or Discover credit or debit card and a 4-digit value on an American Express credit or debit card that provides additional security against fraud, particularly in the online environment.

Airbnb has not adopted FIDO, W3C, SRC, or CoF tokenization. However, it is a good candidate for all of these solutions, particularly CoF tokenization, given its large number of accounts. However, the challenge with CoF tokenization is that markets are in different states of maturity and FIs must all update their proprietary fraud models to evaluate tokenized transactions differently than PAN-based transactions. As a result, authorization rates may be inconsistent across FIs, thereby limiting CoF tokenization adoption.

Card Networks

The card networks' objective is to bring the respective EMV protocols together from a product perspective (e.g., SRC, 3DS, and tokenization) to facilitate industry adoption and achieve scale. SRC went live in the fourth quarter of 2019 and is realizing some initial adoption, but the value of SRC for merchants will depend on the use case. The specification was designed to reduce the number of steps a customer must complete during guest checkout. Mastercard is working with the payment gateways to prepare them for SRC adoption and also reported overall improvements with authorizations for EVM 3DS.

Alternative Authentication Solutions and Tokenization

The panelists also discussed alternative authentication solutions in lieu of these protocols. Netflix leverages its 30-day free membership trial as an opportunity to prevent fraud. The company also uses internal and external data, including device data, to help mitigate fraud.

Airbnb uses device signals, carrier data, and behavioral pattern analysis to help eliminate risk.

Mobile device authentications solutions are considered strong and reinforce the industry desire to move away solely from usernames and passwords, which expose merchants to account takeover. The use of these "new" protocols, in addition to tokenization in a layered approach, create an opportunity to perform better identity verification. Other tools help manage access to consumer accounts, such as challenge questions when a user tries to change the shipping address, or account updater services offered by the card networks that provide updates on cards that are lost, stolen, or expired.

VI. Mobile/Digital Payment Adoption Trends/Insights

Conrad Sheehan of Accenture reviewed the opportunity in the growth of digital commerce. Accenture research indicates that overall global e-commerce sales are forecast to grow from $2.4 trillion in 2017 to $6.5 trillion by 2023, while physical location sales are forecast to grow from $20.5 trillion in 2013 to 29.7 trillion by 2023. Their research has also found that payments are now more than a financial services product. Financial institutions no longer dominate the industry with the entrance of large technology companies, such as Google, Tencent, Ant Financial, Airbnb, Starbucks, Amazon, Uber, and others.

Digital Payments Expansion: A Shifting Environment

The expansion of mobile wallets and alternative checkout solutions (e.g., buy online, pick up in-store) has been well-received by consumers. Over the past decade, the industry has evolved from digital payment *platforms* (e.g., PayPal, Square, Apple Pay, Google Pay, and Samsung Pay) to digital payment *ecosystems* (e.g., Amazon, Airbnb, Starbucks, Uber, Alipay, Google, Apple, and WeChat). Alipay now has over 1 billion users. Uber added 900,000 small business drivers globally in 2019. Starbucks reports that over 35 percent of its transactions are via the Starbucks mobile app.

Today, China is a major player in the payments industry as mobile payments represent 85 percent of its payment volume. In 2015, Ant Financial's AliPay achieved $14 billion in purchase volume in 24 hours–this took eight years for PayPal and two years for Square to achieve.

Europe is also experiencing a shift from the physical POS environment to the e-commerce environment. Many POS payments are moving to mobile apps, particularly for quick-service restaurants that can be ordered ahead and picked up in-store. This shift to mobile apps reflects the appreciation for the convenience and experience that it affords.

The 2019 Federal Reserve Payments Study showed that 49.9 percent of U.S. card spend by value is remote and 50.1 percent is in-person transactions.[60] Most of the U.S. still relies on a POS embedded architecture, but it may be seeing an inflection point as the transportation sector moves toward broader adoption of open payments, including contactless payment adoption.

Other Payments Innovations

Banking as we know it is changing as fintechs are offering innovative payment solutions that leverage the banking infrastructure. Open banking and PSD2 pose interesting possibilities, but raise questions about realistic adoption in the future. In the U.S., screen-scraping solutions offer glimpses into how open banking might evolve, but the market tends to favor innovation versus regulatory-driven initiatives.

Industry adoption of the *International Standards Organization (ISO) 20022 – Universal financial industry message scheme*[61] will profoundly affect the global payments environment. For example, every new RTP system developed will be ISO 20022 compliant. This standard seeks to harmonize information at the core settlement layer and allow for many more data fields, which will prompt more innovation.

VII. Future Considerations

1. Mainstream adoption of blockchain, DLT, and cryptocurrencies

These technologies are moving beyond nascent curiosity. The groundwork is in place for more mainstream adoption of blockchain, digital assets, and cryptocurrencies, but it remains uncertain as to when cryptocurrencies will move into the realm of everyday payments. Scaling remains one of the biggest hurdles to future adoption.

The challenge to widespread adoption for blockchain may be its need for verification of the information going into a blockchain. While this technology creates an immutable source of truth once the information is placed into a block, it does not validate the source information in the first place. Therefore, processes are needed to ensure the accuracy of information going into a blockchain.

The use of blockchain lacks active use cases in mobile and digital payments. However, it may be able to support stronger security based on an immutable database for personal user data and the potential to easily track illegitimate transactions. Blockchain-powered mobile payments can also support the use of tokens

---

[60] U.S. Board of Governors of the Federal Reserve System. (2019). *The 2019 Federal Reserve Payments Study*. Retrieved from https://www.federalreserve.gov/paymentsystems/2019-December-The-Federal-Reserve-Payments-Study.htm.

[61] ISO 20022 is an ISO standard for electronic data interchange between financial institutions. It supports a metadata repository containing descriptions of messages and business processes, and a maintenance process for the repository content. The standard covers financial information transferred between financial institutions, such as payment transactions, securities trading and settlement information, and credit and debit card transactions.

rather than payment credentials, making transactions more secure. Finally, blockchain-based apps can support retailer loyalty programs, using tokens that can be redeemed for purchases.

These technologies remain immature, and would greatly benefit from established standards. Looking ahead, integration with law, regulation and governance will be critical.

2. Modernization of payments is a global theme

Modernization of payments is a global theme, whether it involves faster payments, blockchain, cryptocurrency, stablecoins, P2P payments, or stronger security solutions.

As an increasing number of faster payments solutions are introduced into the U.S. market, and the volume of transactions processed through these solutions grows, the question remains whether the use cases for faster payments present enough value to foster broad-scale adoption.

The mobile payments industry has evolved considerably over the last decade and overcame significant barriers and challenges, while expanding into the digital environment. Today, mobile payments may be considered mainstream even though adoption is slow, because mobile is becoming a platform for new use cases. What does this evolution mean for the future of mobile/digital payments and what will be the next big development in this evolution?

U.S. payments are undergoing a transformation with rapid technology innovation, cloud adoption, and the demand for smarter, faster payments. The global COVID-19 pandemic is accelerating this transformation as more consumers are relying on contactless payments and using less cash, but the question is whether or not it will be sustainable.

3. Mobile P2P: Ensuring consumer confidence & protection

The current mobile P2P landscape is fragmented, offering a wide range of solutions whether FI-based, offered by a third-party provider, or a social media platform. To address the lack of standardization in the U.S. market, the Accredited Standards Committee (ASC) X9 is developing a five-part standard for mobile financial services, for which Part 4 addresses mobile payments to persons.[62]

The growth of mobile P2P dictates the need for more effective education for consumers to understand how these payments work, and their rights and responsibilities. Making consumers aware that they need to ensure the accuracy of the intended recipient's email or mobile number before releasing funds is a critical message. Consumers may also need further education to better understand what is meant by faster payments and how transfer times may vary for certain mobile P2P payments.

4. Authentication and fraud mitigation in the digital environment

Many providers are seeking to create better and more innovative solutions for authentication, data security and fraud prevention in the digital environment, particularly now that chip cards have provided higher

[62] ASC X9 is accredited by the American National Standards Institute (ANSI) to develop and maintain voluntary consensus standards for the financial services industry. For more information, see https://x9.org/.

security at the POS environment. However, these solutions need to be frictionless and not impact the consumer shopping experience.

Several organizations are working to enhance the security of the digital or online commerce channel with stronger authentication approaches. Stronger authentication is needed as the industry seeks to reduce usernames and passwords as the primary authentication method and leverage the use of more data, including biometrics, to verify identities and reduce fraud risk. While the European Union has mandated stronger authentication under PSD2, the U.S. has several industry organizations working to offer stronger solutions by reducing the entry of the PAN, using tokenization, leveraging APIs, and leveraging more data to verify the parties to a transaction.

The current landscape creates a lot of uncertainty around what stakeholders need to do to implement new protocols, such as EMV 3DS and the ability to share more data. The next year will reveal whether or not the industry is creating a more secure online commerce environment as more retailers adopt newer solutions.

Across the payments fraud landscape, industry stakeholders are relying on use of more data to inform risk decision-making as well as artificial intelligence and machine learning tools. More data about the consumer, their mobile device, and shopping behavior can greatly enhance fraud mitigation and help to verify the customer and further distinguish between legitimate and fraudulent transactions. At the same time, increased data capture and analytics raises concerns about data privacy and rights.

5. Industry Engagement and Collaboration

Every participant in the payments system, regardless of its role or its customer base, is faced with the challenge of assessing emerging technologies and developments in fintech to gauge the potential impact on the payments system and its stakeholders. How do we assess the needed level of industry engagement and collaboration to advance the evolution of the U.S. payments system? The MPIW will continue to monitor developments in this area, and where appropriate, facilitate industry collaboration on critical issues.