WAKE FOREST JOURNAL OF BUSINESS AND INTELLECTUAL PROPERTY LAW

VOLUME 17 SUMMER 2017 NUMBER 4

2017 U.S. REGULATORY OVERVIEW OF MOBILE WALLETS AND MOBILE PAYMENTS

Erin Fonte[†]

[†] © 2017 Erin Fonte is a Member and financial services, payments and fintech lawyer with Dykema Gossett PLLC. She is head of Dykema's Financial Services Regulatory and Compliance Group and the FinTech, Payments and Digital Commerce industry group. Her practice includes advising fintech companies, financial institutions, alternative payments providers, vendors and retailers regarding financial services, regulatory and payment systems laws. She regularly advises regarding mobile banking, mobile payments and mobile wallet products and services. Erin also advises advertisers, marketers and retailers/companies regarding add-on mobile products such as mobile loyalty/rewards and geo-location advertising/coupons/offers. Erin has experience with a broad range of matters related to financial technology, banking and financial services, digital commerce, technology/Internet products, privacy and data protection laws, and general corporate matters. She frequently writes and speaks on payments, mobile payments and privacy/data security issues, and was a member of the Federal Reserve's Faster Payments Task Force (2015–2017). She holds a B.A. from U.T. Austin, and received her J.D. (with Distinction) from Stanford Law School. Erin may be reached at efonte@dykema.com, and is also on Twitter: @PaymentsLawyer.

I. INTRODUCTION

One of the buzzwords in financial services is "fintech" (i.e., "financial technology"). Numerous start-ups and venture capital/private equity entities are investing in developing new technologies that seek to "disrupt and disintermediate" traditional financial services.[1] One of the first beachheads in the current fintech invasion is mobile wallets and mobile payments.

"Mobile payments technology is poised to create a dramatically global shift in how individuals pay for goods and services, track spending," interact with retailers, and even manage personal finances.[2] "Mobile payments are also becoming big business for non-financial institution" (non-FI) alternative payments providers.[3] Many of these services offered by non-FIs seek to "disintermediate" traditional banking relationships, creating a fundamental shift in how individuals conduct day-to-day purchasing and interact with their finances.[4]

It was "anticipated that there [would] be more than 4.8 billion individuals using a mobile phone by the end of 2016."[5] "A recent report noted that 39 percent of all mobile users in the U.S. had made a mobile payment in 2015 . . . up from 14 percent in 2014" and usage could reach "the 70 percent range by 2017."[6] Currently, these payments happen in a variety of manners.

Mobile payments have the potential to dramatically affect the world of retailing. Apple Pay and Android pay, examples of digital wallets, are "smart" payment systems that combine payments with two-way, real-time communications.[7] Payments, combined with real-time communication, are promising for retailers because they combine numerous functions such as search functions, payment, advertising, shipping, loyalty programs, and customer service function.[8] Combining all these functions may increase a retailer's ability to

---

[1] *See* Tom C.W. Lin, *Infinite Financial Intermediation*, 50 WAKE FOREST L. REV. 643, 643 (2015).

[2] Erin F. Fonte, *Mobile Payments in the United States: How Disintermediation May Affect Delivery of Payment Functions, Financial Inclusion and Anti-Money Laundering*, 8 WASH. J.L. TECH. & ARTS 419, 421 (2013).

[3] *Id.*

[4] *Id.*

[5] John Rampton, *The Evolution of the Mobile Payment*, TECHCRUNCH (June 17, 2016), https://techcrunch.com/2016/06/17/the-evolution-of-the-mobile-payment/ (alteration in original).

[6] *Id.* (alteration in original).

[7] Adam J. Levitin, *Pandora's Digital Box: The Promise and Perils of Digital Wallets*, 166 U. PA. L. REV. (forthcoming 2017) (manuscript at 1) (on file with Science Research Network).

[8] *Id.*

identify, attract, and retain customers which in turn combines e-commerce and brick-and-mortar platforms.[9]

However, mobile payments also create different risks, then traditional payment methods, for retailers because of the "smart" nature of the payments.[10] Some mobile payments products and services can also reallocate flows of consumer data from merchants to financial institutions (FIs), depriving merchants "of valuable customer information used for anti-fraud, advertising, loyalty, and customer service purposes."[11]

Part II below discusses mobile wallets, mobile payments, and person-to-person (P2P) mobile transfers, including a description of the various mobile payments types, mobile payments products, and how mobile payments technology changes traditional payments transactions. Part III discusses potential risks involved with mobile wallets/mobile payments. Part IV provides a detailed overview of the regulatory framework that currently governs mobile payments in the United States. This article does not touch upon the current and emerging cutting-edge technologies of wearables and connected Internet of Things devices that are being used for payment functionality. Those technologies are also developing at a rapid pace, but in many ways the resulting payment applications are being built upon the "new rails" of mobile payments products and systems discussed in this article.

II. MOBILE WALLETS, MOBILE PAYMENTS, AND P2P TRANSFERS

A. Mobile Banking v. Mobile Wallets/Mobile Payments

The novelty of mobile technology and payment services provided by non-FIs understandably contributes to confusion about the differences between mobile banking and mobile payments. Many FIs offer some combination of online banking services via mobile devices, initially by short messaging service (SMS) that older model "feature" phones use, but now primarily through either a truncated mobile website that operates in a mobile browser, or by a native on-device mobile application (mobile app).[12] Common mobile banking services now include the following traditional online banking functions, along with some new features:

---

[9] *Id.*
[10] *Id.*
[11] *Id.* (manuscript at 1).
[12] Erin F. Fonte, *Overview of Mobile Payments in the United States*, 32 BANKING & FIN. SERVS. POL'Y REP. 1, 2 (2013).

- Account balance inquiries and statement information;
- Bill payment services;
- Traditional funds transfer services (i.e., between accounts)
- Branch and automated teller machine (ATM) location services
- Transaction alerts based on dollar thresholds or other user-established parameters
- Mobile remote deposit check capture services (i.e., "check deposit by phone")[13]

By contrast, we may refer to mobile payments as a term that includes payments services and products offered not just by FIs, but also by emerging and alternative non-FI payments providers as well, such as PayPal (offering a non-FI account that processes and settles transactions between buyers and sellers), Boku (allowing payment for goods and services by charging to a mobile phone bill, which the customer chooses how to settle and pay), or Square (alternative credit/debit card processing service and technology using a mobile device to process payments for small merchants).[14]

Traditional FIs are also innovating in the mobile banking space, as some FIs like JPMorgan Chase, Chase Pay, and Capital One, Capital One Wallet, are offering mobile wallet products.[15] However, non-FIs are leading the development and introduction of a myriad of other new products in the mobile payments space.[16]

B. Mobile Payment Types and Products

There are currently three basic types of mobile payments transactions:

[13] *See id*.

[14] *Id*. at 3; John Stewart, Jim Daly & Linda Punch, *Annual Field Guide to Alternative Payments*, DIGITAL TRANSACTIONS (May 1, 2011), http://www.digitaltransactions.net/news/story/3092.

[15] Fonte, *supra* note 12, at 4.

[16] *See Innovations in Mobile Payment: The Future is Fintech*, BNY MELLON 1, 2 (Oct. 2015), https://www.bnymellon.com/_global-assets/pdf/our-thinking/innovation-in-payments-the-future-is-fintech.pdf.

> ● Mobile commerce transactions utilize a mobile internet browser to perform standard e-commerce transactions;
>
> ● Mobile payments transactions use either some unique technology form factor (such as near-field communication (NFC) or barcode technology like the Starbucks mobile app), or in-app payment functionality (like a "buy" button) to initiate authorization and payment; and
>
> ● Mobile wallets seek to replace an individual's full "wallet" of payment options by storing payment card and payment account credentials and then leveraging one of the various technological form factors to initiate authorization and payment.[17]

The majority of mobile payments conducted today that are not mobile commerce (i.e., just web commerce conducted via mobile device browser) fall into three types of mobile payments services.[18]

1. Digital Wallets

A "digital wallet" typically refers to a payment service that provides:

1. a smartphone app for making financial transactions at a merchant's physical point of sale;[19] and/or

2. a desktop app for making credit/debit/Automated Clearing House (ACH) purchases online.[20] The app eliminates entering shipping, billing, and credit card data when a purchase is made on a website.[21] Data may reside on a user's computer, where it is encrypted, or on the cloud, and the wallet's digital signature is used to identify the cardholder.[22] Store loyalty cards, drivers' licenses, insurance cards, and site passwords can also be stored in a digital wallet.[23] Mobile wallets may also all a user to enter additional data

[17] *See* Fonte, *supra* note 12, at 3–5.
[18] *See* Rampton, *supra* note 5.
[19] *Definition of: Digital Wallet*, PC MAG., http://www.pcmag.com/encyclopedia/term/41399/digital-wallet (last visited Aug. 6, 2017).
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*

other than those enumerated.[24]

An example of a general-use digital wallet that can be used in both e-commerce/mobile commerce via the Internet, or via physical point-of-sale systems is MasterCard's Masterpass.[25]

2. Mobile Wallets

A "mobile wallet" typically refers to a service that enables payment at a physical point of sale via a mobile device.[26] A smartphone wallet app is typically capable of storing multiple payment account credentials (e.g., credit card, debit card, prepaid card, ACH), and employs various user authentication methods and technology to initiate payment transactions.[27] As of the writing of this article, Apple Pay, Android Pay, and Samsung Pay are mobile wallet services currently operating in the United States.[28]

3. P2P Transfers

Mobile P2P transfers are a type of mobile payment that are also a subset of "account-to-account" transfers, whereby transfers are made directly between the sender's and receiver's bank accounts (as opposed to using credit, debit, or prepaid card accounts).[29] Typically, P2P transfers utilize already existing retail payment systems (such as the debit card rails or the ACH rails) to deposit and withdraw funds.[30]

---

[24] *Id.*

[25] *See Masterpass by Mastercard*, MASTERCARD, https://masterpass.com/en-us/ (last visited Aug. 14, 2017).

[26] *See Mobile Wallet Basics*, WELLS FARGO, https://www.wellsfargo.com/mobile-payments/mobile-wallet-basics/ (last visited Aug. 14, 2017).

[27] *See id.*

[28] *See* Todd Hasselton, *Say Goodbye to Your Debit Card: Here's How to Use Your Phone to Pay at the Store*, CNBC (May 6, 2017, 4:14 PM), https://www.cnbc.com/2017/05/06/how-to-use-apple-pay-android-pay-samsung-pay.html.

[29] *See* Oz Shy, *Account-to-Account Electronic Money Transfers: Recent Developments in the United States*, FED. RES. BANK BOS. 1–2 (Oct. 12, 2011), https://www.bostonfed.org/publications/public-policy-discussion-paper/2011/account-to-account-electronic-money-transfers-recent-developments-in-the-united-states.aspx.

[30] *See Online Person-to-Person (P2P), Account-to-Account (A2A) Payments and Electronic Cash*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/payment-instruments,-clearing,-and-settlement/card-based-electronic-payments/online-person-to-person-(p2p),-account-to-account-(a2a)-payments-and-electronic-cash.aspx (last visited Aug. 6, 2017).

The simplest case is when the payor and the payee maintain accounts at the same FI.[31] This type of payment is called an "on-us" or "book" transaction.[32] These transactions are settled by posting accounting entries on the books of one FI.[33] P2P transfers also may occur between individuals at different FIs, which typically settle either through ACH or debit card rails.[34] As technology advances, the transfer of funds through the use of proximity devices, such as mobile devices, is increasing.[35] Examples of current P2P products within the United States are Venmo (owned by PayPal), Zelle (owned by Early Warning and involving major U.S. banks), Dwolla, and Square's Square Cash feature supporting mobile P2P payments.[36]

C. How Mobile Wallet/Mobile Payments Technologies Change Traditional Payments Transactions

Mobile wallets/mobile payments change traditional payments transactions in that instead of having to use a physical plastic credit, debit, or prepaid card (either magnetic stripe or Europay, MasterCard, and Visa (EMV) chip), the payment credentials for the underlying credit, debit, or prepaid card or bank account are stored and transmitted either by the user's digital wallet (with payment credentials typically securely stored in the cloud) or from the user's mobile device (where payment credentials are stored in encrypted form, often using proxy tokens or some other form of tokenization of underlying payment account information).[37] For physical point-of-sale mobile payments, payment credentials are transmitted from consumers to merchants at the point of sale using a variety of different technologies. Several of the technologies described below implement measures to take the payment credential account number, often

[31] *Id.*
[32] *See id.*
[33] *Id.*
[34] *See* Hasselton, *supra* note 28, at 2–3.
[35] *See id.*
[36] *See* Lou Grilli, *P2P – A Comprehensive Look at Person–To–Person Payments*, PAYMENTS REV. (Jan. 12, 2017), http://www.thepaymentsreview.com/a-look-at-p2p-payments.
[37] *See Mobile Wallet Technology*, CHASE, https://www.chasepaymentech.com/mobile_wallet_technology.html (last visited Aug. 14, 2017); Oren Levy, *Europay, Mastercard, Visa: A Primer*, TECHCRUNCH (May 12, 2015), https://techcrunch.com/2015/05/12/europay-mastercard-visa-a-primer/; Susan Pandy, Marianne Crowe & Brian Russell, *Understanding the Role of Host Card Emulation in Mobile Wallets*, FED. RES. BANK BOSTON 1, 1 (May 10, 2016), https://www.bostonfed.org/publications/payment-strategies/understanding-the-role-of-host-card-emulation-in-mobile-wallets.aspx.

referred to in the industry as the primary account number (PAN), out of the payment initiation, authorization, and settlement process to make payment credentials more secure by reducing the ability to hack and capture "live" or actionable payment account information.[38] Without full payment account information, it is much more difficult for fraudsters to either fully clone a payment account or to use the underlying payment account and associated personal information to commit identity theft.[39]

For example, several NFC-based mobile wallet/mobile payments products utilize proxy tokens that do not contain full payment account information, but can be utilized by a trusted third party to re-associate the low-value proxy token (i.e., one with no live payment account information) with the user's actual payment account information.[40] This is essentially how Apple Pay works. When a user provisions his or her payment account to Apple Pay and then uses Apple Pay at the physical point of sale, the information stored in the "secure element" within the iPhone is not actual payment account data, but rather is a "device primary account number" (DPAN) issued by the card network for that particular card to Apple.[41]

When the DPAN is presented at the merchant's NFC-enabled device at the point of sale, the merchant sends the DPAN to the card network (e.g., MasterCard or Visa), and the card network then re-associates the DPAN with the actual PAN for the payment card, sends the authorization request to the card issuing FI for authorization, and then transmits an approved authorization request back to the merchant.[42] The merchant never has the PAN, and the issuing bank never has the DPAN—the card networks, as the "tokenizers," are the only entity able to associate the DPAN proxy with the actual PAN on

[38] *See Tokenization Product Security Guidelines*, PCI SECURITY STANDARDS COUNCIL 1, 75 (Apr. 2015), https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf.

[39] *See generally id.* at 75 (providing that the goal of tokenization is to create a token that has no value to an attacker).

[40] *See* Pandy et al., *supra* note 37, at 1 n.2; Sharon Profis, *Everything You Need to Know About NFC and Mobile Payments*, CNET (Sept. 9, 2014, 12:00 PM), https://www.cnet.com/how-to/how-nfc-works-and-mobile-payments/.

[41] *See Apple Pay Security and Privacy Overview*, APPLE, https://support.apple.com/en-us/HT203027 (last visited Aug. 13, 2017); Erin Fonte, *Apple Pay Wants to be the Apple of Your Bank's Eye*, BANKERS HUB 1, 3 (Dec. 2014), http://173.201.144.147/Newsletters/BankersHub%20Newsletter%20December%202014%20Fonte.pdf.

[42] *See Apple Pay Security and Privacy Overview*, *supra* note 41.

the payment account.[43]

The issue of tokenization and the various approaches and technologies around security of payment account information could easily fill numerous articles, but suffice it to say that for purposes of understanding mobile wallet/mobile payments technology, one of the key selling points to issuing banks, merchants, and consumers is that, in theory, mobile payments technologies should be able to significantly reduce, if not altogether eliminate, the instances when "live" payment account information is present (in either encrypted or unencrypted form) at every stage of transaction initiation, authorization, and settlement.[44]

1. Method of Transmission of Payment Authorization Data from Consumers to Merchants in Mobile Payments Technologies

1. Near Field Communication

NFC is a wireless transmission protocol that allows for encrypted exchange of payment credentials and other data at close range whereby a point-of-sale device "reads" the payment account credentials when the user either swipes or taps his or her NFC-equipped mobile device on the NFC reader present on the NFC-enabled point-of-sale device.[45] NFC utilizes a "secure element" to store the consumer's payment credentials on the consumer's mobile device for access and use at the physical point of sale.[46] Examples of mobile wallets/mobile payments that use NFC technology include Apple Pay, Android Pay, and Samsung Pay.[47]

In the United States, there are currently three models that leverage NFC technology to support contactless mobile wallets:

- "NFC with secure element (SE)"[48]

[43] *See* Marianne Crowe et al., *Is Payment Tokenization Ready for Primetime?*, FED. RESERVE BANK BOS. 1, 6–7 (June 11, 2015), https://www.bostonfed.org/-/media/.../PaymentStrategies/tokenization-prime-time.pdf.

[44] *See* Pandy et al., *supra* note 37.

[45] *See id.* at 1, n.1; Crowe, et. al., *supra* note 43, at 23, 40.

[46] *See* Pandy et al., *supra* note 37, at 1 n.2.

[47] Rampton, *supra* note 5.

[48] Pandy et al., *supra* note 37, at 1 n.2 ("GlobalPlatform defines a secure element (SE) as a tamper-resistant one-chip secure microcontroller capable of securely hosting applications and their confidential and cryptographic data (e.g. key management). In payment applications, the SE controls interactions between trusted sources (bank) and trusted applications (mobile payments app) stored on the SE and

continued . . .

> ● "NFC with host card emulation (HCE) software that replaces the SE in the mobile device to enable the NFC wallet app to perform card emulation."[49]
>
> ● "NFC with a trusted execution environment (TEE), a secure area of the main processor in the mobile device that stores a payment token"[50]

The three technologies mentioned above are used by Apple Pay, Android Pay and Samsung pay—ApplePay stores payment tokens in the mobile device SE, the first model mentioned above, Android Pay uses HCE to store tokens in the Android KitKat v4.4 (or higher) mobile OS, similar to the second model mentioned above, and Samsung Pay uses NFC and HCE, but stores the payment token and cryptographic keys in the TEE in the mobile devices, similar to the third model described above.[51]

2. Cloud Based

Cloud-based mobile payments technology differs from physical element-based payment technology (such as NFC described above), and leverages mobile connection to the Internet to obtain payment credentials (including tokens) that are stored in the cloud and controlled by a trusted third party, rather than stored on the mobile device itself.[52] For example, with mobile apps, payments occur on a consumer's device in order to purchase goods from a specific retailer, such as the Starbucks mobile app that generates a static (i.e., unchanging) bar code that is scanned at the point of sale for each

---

third parties (merchant the user is paying). The secure domain protects the user's credentials and processes the payment transaction in a trusted environment. There are three types of SE's—Subscriber Identity Module (SIM)/Universal Integrated Circuit Card (UICC), micro SD, and embedded secure element (eSE).").

[49] *See id.* at 1 n.3 ("The term 'host card emulation' (HCE) was introduced in 2012 by SimplyTapp to describe the ability for a mobile wallet app to communicate through the NFC controller to a contactless NFC-enabled POS terminal/reader to pass payment card credentials (or payment token), eliminating the need for a physical SE managed by the mobile network operator (MNO). Research in Motion (RIM) had previously implemented a similar process on its Blackberry Bold 990 device in 2011, referring to it as 'virtual target emulation.'").

[50] *Id.* at 1. The term "payment tokens" refers to tokens as defined under the *EMV Payment Tokenization Specification*. *Payment Tokenisation*, EMVCO (Mar. 10, 2014), http://www.emvco.com/specifications.aspx?id=263.) Also, for more information about the tokenization and the difference between security (acquirer/processor) and payment tokenization (network/issuer), *see Tokenization Product Security Guidelines*, *supra* note 33, at 5.

[51] Pandy et al., *supra* note 37, at 2.

[52] *See id.* at 5.

payment transaction.[53] The static bar code is stored within the Starbucks mobile app on the user's mobile device.[54] Some mobile payment technologies that are cloud-based use "dynamic" bar codes that are unique to every transaction, but are still tied back to the user's payment account information.[55] QR Pay is one example of a company that provides an application program interface (API) functionality to generate dynamic bar codes.[56]

3. Proximity-Based

Proximity-based payments utilize geolocation services to initiate payments.[57] In cloud-based proximity payments, merchants are able to find users within range and verify their identity, and their credentials (both customer identity verification and payment credentials) are stored in the cloud.[58] In Bluetooth Low Energy (BLE) proximity payments, "triggering" takes place on either the consumer's or merchant's device where data is stored in a mobile payment account.[59] Examples of BLE-enabled mobile payments include PayPal Beacon and Apple's iBeacon.[60]

4. Mobile P2P

A mobile P2P payment initiated on a mobile device can use a recipient's e-mail address, mobile phone number, or other identifier to initiate payment.[61] Transfer of funds occurs via ACH, card networks, or intra-FI account transfer (i.e., "book" transfer). Venmo, a mobile

[53] *See* Fonte, *supra* note 12, at 3.

[54] *See id.*

[55] *See* Pandy et al., *supra* note 37, at 7.

[56] *See Welcome to QR Pay*, QR PAY, http://qrpal.com/ (last visited Aug. 15, 2017); QR PAY, http://www.qrpay.com/qr-pay (last visited Aug. 15, 2017).

[57] *See Security of Proximity of Mobile Payments*, SMART CARD ALLIANCE 1, 3 (May 2009), https://www.securetechalliance.org/resources/pdf/Security_of_Proximity_Mobile_Payments.pdf.

[58] *See* Massimo Pellegrino et al., *Mobile Proximity Payments – 5 Things Retailers Should Know*, PWC 1, 6 (2016), https://www.pwc.com/it/it/publications/assets/docs/mobile-proximity.pdf.

[59] Rampton, *supra* note 5.

[60] *Id.*

[61] *Appendix E: Mobile Financial Services*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL 1, 3 (Apr. 2016), https://www.ffiec.gov/press/PDF/FFIEC_booklet_Appendix_E_Mobile_Financial_Services.PDF. *See, e.g.*, *Make and Share Payments*, VENMO, https://venmo.com/about/product/ (last visited Aug. 14, 2017) (stating that payments can be made using an email address or phone number).

P2P transfer service acquired by PayPal, reported transferring more than one billion dollars of P2P transactions in January 2016 alone.[62] Meanwhile, major banking institutions, such as JPMorgan Chase & Company, Bank of America Corporation, Wells Fargo & Company, and U.S. Bancorp, have created a joint venture called Zelle (now operated by Early Warning) that allows customers to transfer funds instantly to another bank account through their mobile devices.[63] While the technology for mobile P2P transactions is not particularly complex, technology and security infrastructure must be in place for the P2P transfer system to work and to prevent fraudsters from gaining access to the "directory" that ties personal identifiers to bank account information.

III. RISKS INVOLVED WITH MOBILE WALLETS/MOBILE PAYMENTS

A. Cost of Payments

Whether mobile wallet/mobile payments and P2P transactions will ultimately be more or less costly than traditional methods of payments, which theoretically should have less expensive transaction costs, is a matter for speculation. For example, even though in theory the costs of mobile payments should be lower due to banks not having to issue plastic cards (which are even more costly if they are outfitted with an EMV chip), card networks such as MasterCard and Visa were reportedly charging significant "tokenization" fees for issuing DPANs for NFC mobile wallets, such as Apple Pay.[64] While systems that

[62] Rampton, *supra* note 5.

[63] *See* David Henry & Anna Irrera, *U.S. Banks Launching Answer to Peer-to-Peer Payment App Venmo*, REUTERS (June 12, 2017, 8:06 AM), http://www.reuters.com/article/us-usa-banks-payments-zelle-idUSKBN1931C2; Stacy Cowley, *Cash Faces a New Challenger in Zelle, a Mobile Banking Service*, N.Y. TIMES (June 12, 2017), https://www.nytimes.com/2017/06/12/business/dealbook/mobile-banking-zelle-venmo-apple-pay.html.

[64] *See Mobile Payments: Risk, Security and Assurance Issues*, ISACA 1, 8 (Nov. 2011), http://www.isaca.org/groups/professional-english/pci-compliance/groupdocuments/mobilepaymentswp.pdf; Mary J. Hughes, *The U.S. EMV Chip Card Migration: Considerations for Card Issuers*, COMMUNITY BANKING CONNECTIONS, https://communitybankingconnections.org/articles/2016/i1/emv-chip-card-migration (last visited Aug. 14, 2017); Jim Daly, *As Card-Industry Use of Tokens Increases, MasterCard Plans "Digital Enablement" Fees*, DIGITAL TRANSACTIONS (Aug. 14, 2014), http://www.digitaltransactions.net/news/story/As-Card-Industry-Use-of-Tokens-Increases_-MasterCard-Plans-_Digital-Enablement_-Fees-; Jason Parker & Nate Ralph, *Everything You Want to Know About Apple Pay*, CNET (July 14, 2015, 8:00 AM), https://www.cnet.com/news/everything-you-want-to-know-about-apple-pay/.

utilize ACH transaction rails, instead of credit or debit card transaction rails, should theoretically have less expensive transaction costs, the overall cost for processing payments via mobile wallets/mobile payments can remain high due to technology development and security costs for the mobile wallet/mobile payments provider.[65]

In addition, card network association rules leave room for uncertainty regarding whether a mobile payments transaction qualifies as a "card-present" instead of a "card-not-present" transaction. "Card-not-present" transactions are generally more expensive to process in terms of interchange fees as they are viewed as carrying heightened risk, but in reality, it appears that the convergence of technology will mean that the distinction between "card-present" and "card-not-present" transactions with regard to risk profiles will diminish, if not disappear, within a short amount of time.[66] As of the writing of this article, card networks will only recognize a mobile payments transaction as "card-present" if the payment credentials are stored in some form of SE on the mobile device.[67]

B. Fraud and Data Security

Fraud and data security with regard to mobile wallets/mobile payments continues to be a subject for speculation and debate. As with all new and emerging technologies, consumers, issuing FIs, and merchants are wary of the new technology and unknown security risks. However, as mentioned above, there is a compelling argument that mobile wallets/mobile payments will ultimately prove more secure than traditional plastic cards. On one level, a mobile device such as an iPhone that is equipped with Touch ID or other form of biometric recognition allows for mobile wallets/mobile payments to achieve true three-part multifactor authentication.

"Multifactor authentication" is what is currently required by the Federal Financial Institutions Examination Council (FFIEC) for both

---

[65] *See* Fukimo Hayashi & Terri Bradford, *Mobile Payments: Merchant Perspectives*, 99 FED. RES. BANK KAN. CITY ECON. REV. 33, 45–47 (2014), https://www.kansascityfed.org/publicat/econrev/pdf/14q2Hayashi-Bradford.pdf.

[66] *See* Salvatore Scanio & Jason W. Glasgow, *Payment Card Fraud, Data Breaches, and Emerging Payment Technologies*, 21 FIDELITY L.J. 59, 64 (2015); *Blurred Lines: Card Present and Card-Not-Present*, PYMNTS.COM (Feb. 4, 2015), http://www.pymnts.com/company-spotlight/2015/blurred-lines-card-present-and-card-not-present/.

[67] *See* Christopher Cox & Scott Sanchez, *Transforming the Customer Experience: The Promise of Mobile Wallets*, FIRST DATA 1, 7 (2013), https://www.firstdata.com/downloads/thought-leadership/3609_Mobile_Wallets_WP.PDF.

Internet and mobile transactions and services.[68] In October 2005, the FFIEC issued *Authentication in an Internet Banking Environment*,[69] and in June 2011, it issued *Supplement to Authentication in an Internet Banking Environment*.[70] The 2011 guidance established "multifactor" authentication (as opposed to "single-factor" authentication) where FIs were required to have at least two of three forms of user authentication for online banking transactions: (1) what you have (e.g., an ATM card, smart card, or a physical token); (2) what you know (e.g., a password or personal identification number (PIN)); and (3) who you are (e.g., a biometric characteristic, such as a fingerprint).[71] Multifactor authentication requirements have been extended to banking services in the mobile channel as well.[72]

Mobile payments that contain a biometric feature can achieve true three-part multifactor authentication if they combine all three form factors.[73] When you add geolocation information as an additional "fourth" factor in a multifactor authentication environment, then that arguably bolsters difficulty in a fraudster simultaneously faking all four authentication factors at once. When one also considers the fact that mobile payments replace the live and actionable payment account credentials with low value tokens that can only be re-associated with actual payment account data by trusted third parties, it becomes clear that two elements that fraudsters must have—authentication

[68] *See* Press Release, Fed. Fin. Insts. Examination Council, FFIEC Releases Supplemental Guidance on Internet Banking Authentication (June 28, 2011), https://www.ffiec.gov/press/pr062811.htm; *Supplement to Authentication in an Internet Banking Environment*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL 1, 2, 4 (June 28, 2011), https://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf.

[69] *FFIEC Guidance: Authentication in an Internet Banking Environment*, FED. DEPOSIT INS. CORP. (Oct. 12, 2005), https://www.fdic.gov/news/news/financial/2005/fil10305.html. The FFIEC publication (hereinafter *Authentication in an Internet Banking Environment*) is available at https://www.ffiec.gov/pdf/authentication_guidance.pdf.

[70] *See Supplement to Authentication in an Internet Banking Environment, supra* note 68.

[71] *See id.* at 2; *FFIEC Guidance: Authentication in an Internet Banking Environment*, *supra* note 69, at 1, 3; *Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL 1, 6 (Aug. 15, 2006), https://www.ffiec.gov/pdf/authentication_faq.pdf ("By definition true multifactor authentication requires the use of solutions from two or more of the three categories of factors.").

[72] *See Appendix E: Mobile Financial Services*, *supra* note 61, at 10.

[73] *See generally FFIEC Guidance: Authentication in an Internet Banking Environment*, *supra* note 69, at 3 (identifying three basic factors for multifactor authentication).

credentials and actual payment account information—become extremely difficult to obtain.[74]

But extremely difficult to obtain does not mean impossible. Fraudsters can still "phish" or otherwise steal, and fake, all four form factors discussed above.[75] In addition, if the "token vaults" of a trusted third party that re-associates low-value tokens with actual underlying payment account information are ever hacked, then fraudsters would obtain the so called "keys to the kingdom" and could obtain the underlying payment account credentials.[76] While mobile wallets/mobile payments certainly hold the promise of a more secure, less hacker-prone payments process, whether that promise can ultimately be fulfilled is still unfolding in this new environment.

C. Control over Customer Data

In addition to the potential to achieve greater security at a lower cost, merchants are particularly excited about linking mobile wallet/mobile payment to ads, offers, or loyalty/rewards programs.[77] Some retailers, such as Wal-Mart, are now creating their own products, including using geolocation to provide targeted coupons to customers' phones while they shop.[78] Many merchants also use loyalty cards and programs to gather information regarding customer behavior and customer spending, often tying product-level information for each purchase to a particular transaction linked to a loyalty/rewards program customer's account.[79]

---

[74] *See generally* Crowe et al., *supra* note 43 (discussing payment tokens).

[75] *See generally Ask Sucuri: How Modern Web Phishing Works*, SUCURI (Aug. 30, 2016), https://blog.sucuri.net/2016/08/modern-web-phishing-works.html (using malware research to describe the process of online phishing).

[76] *See After a Series of Hacks, Cryptocurrency Issuers May Turn to Old-Fashioned Bank Vaults for Security*, QUARTZ (July 25, 2017), https://qz.com/1036976/after-a-series-of-ethereum-hacks-bitbounce-may-use-a-bank-vault-to-protect-its-ico-tokens/ ("Crypto heists work like this: ether and bitcoin holdings can only be accessed by a private key, a kind of password to a digital currency wallet. The trouble is safeguarding that key: If hackers find a way to steal it, then a digital wallet can be accessed.").

[77] *See* Forbes Finance Council, *Eight Exciting Effects of Mobile Payments Going Mainstream*, FORBES (June 7, 2017, 9:00 AM), https://www.forbes.com/sites/forbesfinancecouncil/2017/06/07/eight-exciting-side-effects-of-mobile-payments-going-mainstream/#201789e24ca2.

[78] Rampton, *supra* note 5.

[79] *See, e.g.*, Thomas H. Davenport, Leandro DalleMule & John Lucker, *Know What Your Customers Want Before They Do*, HARV. BUS. REV. (Dec. 2011), https://hbr.org/2011/12/know-what-your-customers-want-before-they-do (stating that Tesco uses its royalty program to track how customers pay, what they buy, and which store they are purchasing from).

One of the controversies with merchants when Apple Pay launched was that, due to the device-tokenization and the lack of actual primary account number information being passed to the merchant via the Apple Pay transaction (even in truncated form), merchants were no longer able to match particular transactions to particular loyalty/rewards customers due to the lack of that data being passed on to retailers from Apple Pay transactions.[80] Similarly, many mobile payments transaction flows and technologies may disintermediate merchants from transaction data and their ability to associate it with item-level purchase information.[81]

This could be one of the significant reasons why many merchants are implementing in-app payments through the merchant's branded mobile app, which allows continued access to customer data and facilitates specific targeted ads, offers, and loyalty/rewards incentives.[82] Issues surrounding ownership of both transaction information and customer personal information continue to evolve at a remarkable pace, with many players in the payments ecosystem, such as card networks, issuing banks, technology service providers and merchants, trying to exercise sole and exclusive ownership of transaction data and customer personal information—even if another party in the transaction separately obtained, for example, a customer's e-mail address through a loyalty/rewards program.[83] Ownership and use of transaction and personal information data presents distinct issues that must be resolved with customers' underlying privacy rights. However, while these issues remain unresolved, many companies are engaging in a "data grab" to make sure they are not cut out of valuable data streams around mobile payments transactions.[84]

---

[80] *See* Nandita Bose, *Exclusive: In 'Year of Apple Pay', Many Top Retailers Remain Skeptical*, REUTERS (June 2, 2015, 9:05 PM), http://www.reuters.com/article/us-apple-pay-idUSKBN0OL0CM20150606.

[81] *See id.*

[82] *See* Michelle Saettler, *How Merchants Tie Loyalty to Mobile Wallets and Drive Results*, RETAILDIVE, http://www.retaildive.com/ex/mobilecommercedaily/how-merchants-tie-loyalty-to-mobile-wallets-and-drive-results (last visited Aug. 15, 2017).

[83] *See* Tamara Dull, *Who Owns the Data? Well, it's Complicated*., SAS CONSUMER INTELLIGENCE BLOG (Sept. 26, 2014), http://blogs.sas.com/content/customeranalytics/2014/09/26/who-owns-the-data-well-its-complicated/.

[84] *See* Kashmir Hill, *How Target Figured Out a Teen Girl was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012, 11:02 AM), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#6a4fb28a6668.

D. Intellectual Property Issues

Due to the fact that mobile wallets/mobile payments involve not only payments technology but also mobile phone technology and mobile app/user interface development—not to mention hosted services and cloud computing in the background—there are a number of intellectual property (IP) issues and potential claims that can arise for developers and users of mobile payments technologies.[85] This article does not have room for a detailed discussion of all the IP issues that can arise, but mobile wallet/mobile payments providers that may wish to disclaim all warranties of non-infringement or disclaim any liability or indemnification for third-party claims of infringement may find significant pushback from merchants on these IP issues, with many demanding either a warranty of non-infringement or indemnification for third-party IP infringement claims at the very least.[86]

IV. REGULATORY FRAMEWORK

Mobile wallet/mobile payments products and services can trigger a surprising number of potentially applicable laws, rules, and regulations because the services touch upon financial services laws, mobile phone/device laws, and privacy/data security laws.[87] In addition, there are card network (e.g., American Express, Discover, MasterCard, Visa) and private network (e.g., National Automated Clearing House Association (NACHA)) rules and requirements governing these transactions as well.[88] This section reviews potentially applicable laws and the regulatory framework in four areas: (1) transactions; (2) privacy/data security; (3) consumer protection; and (4) other miscellaneous regulatory requirements. The discussion below

[85] *See* James Wester, *Mobile Payments Become Patent Battleground*, MOBILE PAYMENTS TODAY (Feb. 20, 2012), https://www.mobilepaymentstoday.com/articles/mobile-payments-becomes-patent-battleground/.

[86] *See* Jeffrey B. Fabian, *Warranties of Noninfringement and Allocation of Infringement Risk*, INSIGHTS (Fall 2014), http://www.slk-law.com/portalresource/lookup/poid/Z1tOl9NPluKPtDNIqLMRVPMQiLsSw4JCv4ZD/document.name=/Warranties%20of%20Noninfringement.pdf.

[87] *See Mobile Payments: An Evolving Landscape*, FED. DEPOSIT INS. CORP. (Winter 2012), https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin12/mobile.html.

[88] *See, e.g.*, *Rules Impacting Processors and Merchants*, MASTERCARD, https://www.mastercard.us/en-us/about-mastercard/what-we-do/rules.html (last visited Aug. 14, 2017); *NACHA Operating Rules*, NAT'L AUTOMATED CLEARING HOUSE ASS'N, https://www.nacha.org/rules (last visited Aug. 14, 2017).

includes applicable federal and state laws, rules, and regulations as well as relevant federal agency guidance.

A. Regulatory Frameworks Governing Transactions

1. Electronic Funds Transaction Act/Regulation E

The federal Electronic Funds Transaction Act (EFTA) and Regulation E establish rules for electronic funds transfers (EFTs) involving consumers.[89] The rights, liabilities, and responsibilities of the FIs and entities who provide EFT services, as well as consumers who engage in EFTs are set out in the EFTA, and its implementing rule, Regulation E.[90] An EFT generally includes any transaction "initiated through an electronic terminal, telephone, computer (including online banking), or magnetic tape that instructs a financial institution either to credit or debit a consumer's account."[91] "Financial institution" is defined under the EFTA as "a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person who, directly or indirectly, holds an account belonging to a consumer . . . ."[92] The term "account" generally means a consumer access account held by an FI and established "primarily for personal, family, or household purposes . . . ."[93]

An entity subject to EFTA and Regulation E must comply with the provisions of the law and regulation, which includes required disclosures to consumers[94] and procedures for consumer notifications and investigation and resolution of alleged fraudulent or unauthorized EFTs within specific timeframes.[95] EFTA and Regulation E also limits consumer liability for fraudulent or unauthorized transactions, with varying limits based upon timing of notification to the FI.[96]

---

[89] Provisions of the EFTA can be found at 15 U.S.C. §§ 1693a–1693p (2012), and provisions of Regulation E can be found at 12 C.F.R. pt. 1005 (2017).

[90] *Compliance Guide for Small Entities*, FED. RESERVE SYS., https://www.federalreserve.gov/bankinforeg/regecg.htm (last updated Dec. 28, 2016). *See* 15 U.S.C. §§ 1693a, 1693b(a); 12 C.F.R. § 1005.3(a) (2013).

[91] 15 U.S.C. § 1693a(7) (definition of "electronic funds transfer").

[92] *Id.* § 1693a(9) (definition of "financial institution").

[93] *Id*. § 1693a(2) (definition of "account").

[94] *See* 15 U.S.C. § 1693c(a) (2012); 12 C.F.R. § 1005.9(a) (2016) (proscribing requirements for receipts at electronic terminals and periodic statements).

[95] *See* 15 U.S.C. §§ 1693f(a)–(d) (2012); 12 C.F.R. § 1005.11 (2016) (setting forth procedures for resolving errors).

[96] *See* 15 U.S.C. § 1693g (2012); 12 C.F.R.§ 1005.6 (2016) (setting forth liability of consumers for unauthorized transfers).

Entities that are subject to EFTA and Regulation E must establish a substantial compliance program to oversee and implement compliance.[97]

Many mobile wallet/mobile payments providers have researched applicable definitions of the EFTA and Regulation E and concluded that they are not covered by the provisions (although they may be subject to the provisions of Reg E "Lite," as discussed below).[98] However, the Consumer Financial Protection Bureau (CFPB) released its final Prepaid Card Rule (clocking in at 1,689 pages) on October 5, 2016, with most provisions of the new rule effective as of October 1, 2017.[99] The final CFPB Prepaid Card Rule expands Regulation E compliance obligations to a variety of prepaid card accounts, including coverage of certain digital wallets and P2P accounts.[100]

> 'The new rule applies to traditional prepaid cards as well as mobile wallets, person-to-person payment products and other electronic accounts that can store funds,' CFPB Director Richard Cordray said during a press conference [October 4th, 2016]. Kristine Andreassen, senior counsel in the CFPB's office of regulations, [sic] clarified this by explaining that mobile wallets that can store funds are covered under the final rule, while those that act simply as a 'pass-

[97] *See* 12 C.F.R. § 1005.33(g) (2016). *See also CFPB Consumer Laws and Regulations: Electronic Fund Transfer Act*, CONSUMER FIN. PROTECTION BUREAU 1, 60 (Oct. 2013), http://files.consumerfinance.gov/f/201310_cfpb_updated-regulation-e-examination-procedures_including-remittances.pdf (outlining EFTA examination procedures).

[98] *See generally Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z)*, CONSUMER FIN. PROTECTION BUREAU 1, 35, 120, http://files.consumerfinance.gov/f/documents/20161005_cfpb_Final_Rule_Prepaid_Accounts.pdf (last visited Aug. 15, 2017) (stating that "the application of FTA and Regulation E to digital and mobile wallets has been less clear than the application of the statute and regulation to prepaid . . . accounts."). *See also infra* notes 105–15.

[99] *See id.*; *CFPB Finalizes Strong Federal Protections for Prepaid Account Consumers*, CONSUMER FIN. PROTECTION BUREAU (Oct. 5, 2016), http://www.consumerfinance.gov/about-us/newsroom/cfpb-finalizes-strong-federal-protections-prepaid-account-consumers/; *Prepaid Rule*, CONSUMER FIN. PROTECTION BUREAU, https://www.consumerfinance.gov/policy-compliance/guidance/implementation-guidance/prepaid-rule/ (last visited Aug. 15, 2017).

[100] *CFPB Includes Mobile Wallets in Final Prepaid Rule*, PAYBEFORE (Oct. 5, 2016), http://paybefore.com/pay-gov/cfpb-includes-mobile-wallets-in-final-prepaid-rule/.

through' are not covered.[101]

The result is that many mobile wallets, like Google Wallet and PayPal's Venmo, have to meet the final rule's requirements, whereas wallets such as Apple Pay are not covered by the revised Regulation E provisions because they only store payment credentials for underlying debit or prepaid accounts issued where funds are held by other entities, rather than storing funds in the mobile wallet provider's account.[102] PayPal and Google objected to the CFPB's inclusion of their mobile wallets on the grounds that they can store funds and do P2P transfers.[103] In 2015, Google "submitted a comment to the CFPB stressing that 'overregulation would unnecessarily stifle this emerging market' for mobile wallets, requesting that the CFPB 'tread lightly' in regulating them . . . ."[104]

Regardless of industry objections, the CFPB did not change its final rule on this issue:

> The Bureau continues to believe that digital wallets that can hold funds operate in large part in a similar manner to physical or online prepaid accounts—a consumer can load funds into the account, spend the funds at multiple, unaffiliated merchants (or conduct P2P transfers), and reload the account once the funds are depleted. Accordingly, the Bureau believes that consumers who transact using digital wallets deserve the same protections as consumers who use other prepaid accounts. Indeed, as with other prepaid accounts, a consumer's digital wallet could fall victim to erroneous or fraudulent transactions.[105]

The final CFPB Prepaid Card Rule arguably applies to providers such as PayPal, owner of Venmo, and banks that use P2P services, such as Popmoney, from processor Fiserv Inc., among others.[106] It remains to

---

[101] *Id.* (alteration in original).

[102] *See id.*

[103] *Id.*

[104] *Id.*

[105] Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z), 81 Fed. Reg. 83934, 83972 (Nov. 11, 2016) (to be codified at 12 C.F.R. §§ 1005, 1026). *See Second Thoughts: CFPB and Prepaid Card Rules*, PYMNTS.COM (June 20, 2017), https://www.pymnts.com/news/cfpb/2017/richard-cordray-and-cfpb-rethinks-prepaid-card-rules/.

[106] Jim Daly, *The CFPB's Final Prepaid Card Rule Raises Concerns About Digital Wallets*, DIGITAL TRANSACTIONS (Oct. 5, 2016), http://www.digitaltransactions.net/news/story/The-CFPB_s-Final-Prepaid-Card-

continued . . .

be seen how extensive the CFPB Prepaid Card Rule's coverage will be. "Everybody involved in bank P2P . . . may have new regs . . . [i]t's hard to tell. There are 1,600 pages here. The rule is so sprawling it's hard to tell where it ends."[107] As of the writing of this publication, many mobile wallet/mobile payments providers are still unclear of the rule's applicability to their products and services.[108]

2. Reg E "Lite"

Even if a mobile wallet/mobile payments provider is not an entity subject to the EFTA and Regulation E under the CFPB Final Prepaid Card Rule, the entity may nevertheless have some EFTA and Regulation E compliance obligations. Regulation E includes provisions that apply specifically to a provider of an "electronic funds transfer service" under 12 C.F.R. § 1005.14.[109] These provisions are colloquially referred to as Reg E "Lite" provisions, and are particularly applicable to mobile wallet/mobile payments providers whose services are deemed to fall within the definition of "access device," thereby triggering application of Reg E "Lite" requirements.[110] Reg E "Lite" applies to any person that "provides an electronic fund transfer service to a consumer but that does not hold the consumer's account . . . ."[111] An entity is subject to the Reg E "Lite" provisions if the person: "(1) Issues a debit card (or other access device) that the consumer can use to access the consumer's account held by a financial institution; and (2) Has no agreement with the account-holding institution regarding such access."[112]

Rule-Raises-Concerns-About-Digital-Wallets.

[107] *Id.* (alteration in original).

[108] *See CFPB Proposes Further Changes to Prepaid Rule; Issues Compliance Guide*, ABA BANKING J. (June 15, 2017), http://bankingjournal.aba.com/2017/06/cfpb-proposes-further-changes-to-prepaid-rule-issues-compliance-guide/ (noting that the CFPB proposed changes and reopened the comment period on June 15, 2017).

[109] *See* 12 C.F.R. § 1005.14 (2017) (specifying when an electronic fund transfer service is subject to the requirements of Regulation E).

[110] *See id.*; 12 C.F.R. § 1005.2(a)(1)–(b)(2) (2016) (defining "access device" and when a payroll card account is included); Mark E. Budnitz, *The Legal Framework of Mobile Payments: Gaps, Ambiguities, and Overlap*, PEW CENTER 1, 10–11 (Feb. 10, 2016), http://www.pewtrusts.org/~/media/assets/2016/02/legal_framework_of_mobile_payments_white_paper.pdf; Elizabeth A. Khalil et al., *In Brief: CFPB Issues Long-Awaited Final Prepaid Rule*, CONSUMER FIN. SERVS. L. BLOG (Oct. 10, 2016), http://www.cfs-lawblog.com/in-brief-cfpb-issues-long-awaited-final-prepaid-rule_101016.

[111] *See* 12 C.F.R. § 1005.14(a) (2017).

[112] *Id.* § 1005.14(a)(1)–(a)(2).

An "access device" is defined as "a card, code or other means of access to a consumer's account, or any combination thereof, that may be used by the consumer to initiate electronic fund transfers."[113] For mobile wallet providers, provisions that apply to providers of an "access device" used to access accounts are particularly important.[114]

Under the broad definition of "access device," mobile wallet/mobile payments services that store payment credentials for debit or prepaid card accounts, and are used to initiate transactions, will be subject to Reg E "Lite" requirements.[115] The Reg E "Lite" provisions contain specific compliance requirements, including:

- Required disclosures and documentation;[116]
- Error resolution (including primary responsibility for investigations of alleged unauthorized or fraudulent transactions, and requirements to work with the account-holding institution or entity for both investigation and the granting of provisional credit to the consumer during the investigation);[117] and
- Final resolution of investigation and transfer funds to or from the consumer's account, in the appropriate amount and within the applicable time period if the investigation concludes that an error occurred for which the consumer is not liable (or has limited liability) under Regulation E.[118]

In summary, the rules of the road regarding EFTA/Regulation E compliance for mobile wallet/mobile payments providers will undergo significant changes over the coming year due to the requirements of the CFPB's final Prepaid Card Rule (provided that the rule survives the Congressional Review Act).[119] Mobile wallet/mobile payments providers are well-advised to review the new rule and to remember that even if they are not subject to full-blown EFTA/Regulation E compliance, they may well be subject to Reg E "Lite" requirements as the provider of an "access device" for originating EFTs.

---

[113] *Id*. § 1005.2(a)(1).

[114] *See* Budnitz, *supra* note 110, at 10–11 (noting the definition of "access device" could cover mobile wallets).

[115] *See id.*

[116] *See* § 1005.14(b)(1).

[117] *See* § 1005.14(b)(2).

[118] *See id.*

[119] *See* 5 U.S.C. §§ 801–808 (2012) (Congressional Review of Agency Rulemaking); *CFPB Proposes Further Changes to Prepaid Rule; Issues Compliance Guide*, *supra* note 108.

3. *EFTA/Regulation E and the Durbin Amendment/Regulation II*

The Durbin Amendment was enacted as part of the Dodd-Frank Wall Street Reform and Consumer Protection Act.[120] It places limits on interchange fees as well as limits the compensation a debit card issuer can receive.[121] These limits apply if the issuer has assets in excess of ten billion dollars.[122] Under Regulation II promulgated under the Durbin Amendment by the Federal Reserve Board, debit cards are broadly defined to include "any code or device (other than paper checks or drafts or facsimiles thereof) issued or approved for use through a payment card network to debit an account."[123] General-use (open-loop) prepaid cards are included in this definition.[124] The issuer of a debit card or prepaid account, included in the Regulation II definition, must enable a minimum of two unaffiliated payment card networks on each debit card.[125] Regulation II also forbids an "issuer or payment card network from directly or indirectly inhibiting the ability of merchants to direct the routing of electronic debit transactions for processing over any payment card network of the merchant's choosing that may process such transactions."[126]

With regard to mobile wallets/mobile payments, the landscape is still evolving as to whether technology and tokenization efforts are enabling or preventing issuers from offering merchants the unaffiliated network routing options as required under Regulation II.[127] Merchants have claimed that, for example, Apple Pay transactions that are tokenized go straight to Visa and MasterCard networks, and merchants

---

[120] *Examining the Extensive Regulations of Financial Technologies*, FIN. INNOVATION NOW 1, 24 (July 2016), https://financialinnovationnow.org/wp-content/uploads/2016/07/Examining_the_Extensive_Regulation_of_Financial_Technologies.pdf. *See* 12 C.F.R. §§ 235.3–.6 (2017); *Durbin Amendment*, NAPCP, http://www.napcp.org/page/DurbinAmendment (last visited Aug. 15, 2017).

[121] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 24.

[122] *Id*.

[123] *Id. See* 12 C.F.R. § 235.2(f) (2017).

[124] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 24. *See* § 235.2(f)(2).

[125] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 24. *See* § 235.7(a)(2) (2011).

[126] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 24–25. *See* § 235.7(b).

[127] *See generally* Joe Adler, *Apple Pay May Reignite War over Durbin Amendment*, AM. BANKER (Apr. 6, 2015), https://www.americanbanker.com/news/apple-pay-may-reignite-war-over-durbin-amendment (discussing merchant routing options).

do not have a choice in routing.[128] However, "[s]ome PIN networks, including STAR and Fiserv's Accel, have already touted their capability to facilitate Apple Pay transactions" and they constitute debit networks that are "unaffiliated" with Visa and MasterCard.[129] As the use of mobile wallets/mobile payments increases, and as both NFC and tokenization technologies continue to evolve, this is an area that may undergo more regulatory scrutiny if merchants are able to show that they are systematically deprived of routing choices with these new technology offerings that are required under the Durbin Amendment/Regulation II.[130]

4. EFTA/Regulation E and the Remittance Transfer Rule

If a mobile wallet/mobile payments provider is involved in facilitating or processing international money transfers, that entity will need to make sure it is in compliance with the CFPB's Remittance Transfer Rule, promulgated by the CFPB, under the EFTA, as an amendment to Regulation E.[131] The Remittance Transfer Rule amended Regulation E, regarding international remittances, to require that companies that make those services available provide additional protections to consumers.[132] Those provisions include disclosure requirements, including foreign currency conversion fees, and provisions for error resolution and cancellation.[133]

The Remittance Transfer Rule also requires the remittance transfer provider to train their staff on policies and procedures and to adopt new forms and disclosures, including mobile and text message disclosures.[134] Any provider of a mobile wallet/mobile payments service that provides for international remittance will be subject to the Remittance Transfer Rule, and must develop disclosures, policies, and procedures, as well as an internal compliance program, to ensure compliance with the rule.[135]

---

[128] *See id.*

[129] *Id.*

[130] *See* Adler, *supra* note 127.

[131] *See* 12 C.F.R. §§ 1005.30–1005.36 (2017); *Electronic Fund Transfers (Regulation E)*; *Amendments*, CONSUMER FIN. PROTECTION BUREAU, https://www.consumerfinance.gov/policy-compliance/rulemaking/final-rules/electronic-fund-transfers-regulation-e/ (last visited Aug. 15, 2017).

[132] *See* §§ 1005.30–.36.

[133] *See* §§ 1005.31, 1005.33, 1005.34.

[134] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 30. *See* §§ 1005.31(a)(5), 1005.35 (prescribing disclosures for mobile application or text message transactions and liability for violations by employees).

[135] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 30. *See* Brad Banyas & Dominic Suszek, *Demystifying the Dodd-Frank*

continued . . .

B. Truth in Lending Act/Regulation Z

The federal Truth in Lending Act (TILA) and Regulation Z, promulgated pursuant to TILA, are intended to establish rules to help consumers understand the cost of credit and compare credit options.[136] TILA and Regulation Z generally apply to "creditors" that offer or extend credit to consumers and include both open-end and closed-end credit products, including credit cards.[137] The purpose of TILA is "to assure a meaningful disclosure of credit terms so that the consumer will be able to compare more readily the various credit terms available to him and avoid the uninformed use of credit, and to protect the consumer against inaccurate and unfair credit billing and credit card practices."[138]

For mobile wallet/mobile payments providers, it is important to note that Regulation Z does not focus on the payment aspect (i.e., the function that provides substantially immediate payment to sellers), but rather the credit aspect (i.e., the commitment by the consumer/purchaser to repay the issuer at some time in the future) of a transaction.[139] If a mobile wallet/mobile payments service offers an extension of credit as defined under TILA or Regulation Z, then these requirements apply (including required disclosures, dispute resolution, investigation, and limitations on consumer liability for fraudulent or unauthorized transactions).[140]

However, most mobile wallet/mobile payments providers currently do not offer extensions of credit, but rather merely store the payment credentials of a credit card account that is issued by an FI.[141] In these instances, the mobile wallet/mobile payments provider will be expected to work with the issuing FI to investigate and resolve claims of unauthorized and fraudulent transactions.[142] Since many mobile wallet/mobile payments providers that store payment credentials often allow use and storage of credit, debit, and prepaid cards, many of these

Remittance Transfer Rule, CUINSIGHT (Jan. 2, 2013), https://www.cuinsight.com/demystifying-the-dodd-frank-remittance-transfer-rule-2.html.

[136] *See* 15 U.S.C. §§ 1601–1666(j) (2012); 12 C.F.R. §§ 226.1, 226.59 (2012).

[137] *See* § 226.1(c); 12 C.F.R. § 226.2(a)(17) (2011). *See also Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 16–17.

[138] 15 U.S.C. § 1601(a).

[139] *See Mobile Payments: An Evolving Landscape*, *supra* note 87 (noting that Regulation Z applies when a credit card is the source of payment).

[140] *See* 15 U.S.C. § 1602.

[141] *See Mobile Wallets: How They Work and are They Safe?*, CAPITAL ONE, https://www.capitalone.com/credit-cards/blog/what-is-mobile-wallet/ (last visited Aug. 15, 2017).

[142] *See generally id.* (discussing the security of mobile wallets).

providers subject to Reg E "Lite" as discussed above also include credit card investigation and dispute resolution in their compliance programs as they are already doing the same for debit and prepaid cards.[143]

C. Truth in Billing Laws

Mobile wallet/mobile payments providers that charge payments directly to a consumer's mobile wireless or mobile carrier account, instead of a debit, credit, or prepaid card or bank account (so-called bill to mobile payment services), must also be aware of the "Truth-in-Billing" requirements of the Federal Communications Commission (FCC).[144] Under Truth-in-Billing requirements, "wireless carriers must provide clear, correct, and detailed billing information to customers . . . [including] a description of services provided and charges made.[145] The Truth-in-Billing requirements apply to wireless carriers, but mobile wallet/mobile payments providers must be aware of the requirements to understand how wireless carriers must handle disclosure and dispute resolution requirements and how the bill to mobile provider must cooperate and assist with wireless carriers in compliance with their Truth-in-Billing requirements.[146]

D. Bank Secrecy Act/Anti-Money Laundering Regulations

The Bank Secrecy Act (BSA) (which includes provisions of the USA PATRIOT Act) and its implementing regulations (collectively referred to as BSA Rules) support government efforts to combat drug trafficking, money laundering, and other crimes such as terrorist financing.[147] The BSA Rules were enacted "to prevent banks and other financial services providers from being used as intermediaries for, or to otherwise hide, the transfer or deposit of money derived from, criminal activity."[148] The BSA Rules set out situations and

---

[143] *See supra* notes 103–13.

[144] *See* 47 C.F.R. §§ 64.2400–.2401 (2016).

[145] *Mobile Payments: An Evolving Landscape*, *supra* note 87 (alteration in original). *See* § 64.2401.

[146] *See generally* § 64.2401 (applying the rules to telecommunications common carriers).

[147] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 12, 25. *See* 31 U.S.C. §§ 5311–5330 (2012); 12 U.S.C. §§ 1829b, 1951–59 (2012); USA PATRIOT Act, 31 U.S.C. § 5312(a)(2) (2012) (adding to the anti-money laundering program); 31 C.F.R. §§ 1010.310–.314 (2016).

[148] DENNIS COX, HANDBOOK OF ANTI-MONEY LAUNDERING 133 (2014). *See, e.g.*, 31 U.S.C. §§ 5313(a), 5318(g).

transactions that must be reported to federal authorities, as well as compliance systems that must be implemented, such as screening customers against the U.S. Department of the Treasury's Office of Foreign Asset Control's sanctions list and Specially Designated Nationals List, which contain countries and individuals barred from doing business with U.S. FIs and other companies.[149]

While some of the functions that processors or mobile wallet/mobile payments providers perform may not fall exactly within the BSA Rules, an entity that processes a credit card or certain types of prepaid accounts (such as gift cards, rewards cards, and other stored-value devices) must comply with the BSA Rules and is subject to enforcement actions by the U.S. Department of the Treasury and the U.S. Department of Justice.[150] Payment processors and mobile wallet/mobile payments providers should maintain thorough compliance programs to assure they conform to BSA Rules, as well as related requirements imposed by contract with any partnering FIs or networks, including card association or card network rules.[151]

A processor or mobile wallet/mobile payments provider that is partnering with an FI may be deemed by regulators to be a "service provider" to that FI, and therefore may be subject to "pass through" requirements imposed via contract by the FI as part of the FI's third party vendor management (which also applies to any service providers a vendor).[152] These requirements are designed to ensure that the service provider is conducting appropriate customer due diligence and transmitting appropriate information to allow the FI to meet its

[149] *See Examining the Extensive Regulations of Financial Technologies*, *supra note* 120 at 12, 21, 25; *Office of Foreign Assets Control – Overview*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_037.htm (last visited Aug. 16, 2017); *Anti-Money Laundering (AML) Source Tool for Broker-Dealers*, SEC. & EXCH. COMM'N (Jan. 11, 2017), https://www.sec.gov/about/offices/ocie/amlsourcetool.htm#1; *BSA and Related Regulations*, OFF. COMPTROLLER CURRENCY, https://www.occ.treas.gov/topics/compliance-bsa/bsa/bsa-regulations/index-bsa-regulations.html (last visited Aug. 16, 2017).

[150] *Examining the Extensive Regulations of Financial Technologies*, *supra note* 120, at 25. *See Bank Secrecy Act/ Anti-Money Laundering Examination Manual*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL 1, 4–5, 9, 137, 227 (Feb. 27, 2015), https://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014_v2.pdf.

[151] *See Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 25; *Bank Secrecy Act/ Anti-Money Laundering Examination Manual*, *supra* note 150 at 229, 236–38.

[152] *See Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 26.

obligations under the BSA Rules.[153] FIs will also often require what is colloquially referred to as "fourth-party due diligence" whereby a service provider contractually requires its own vendors and subcontractors to follow all the requirements that the company itself must meet as a service provider.[154]

1. Customer Identification Program Requirements

The USA PATRIOT ACT empowers the Secretary of the Treasury to set out minimum standards that require a FI to validate the identity of an entity or any person who wants to open an account with the FI.[155] These standards are known as the "Customer Identification Requirements" (or CIP Rules), which require FIs to implement reasonable procedures to: (1) verify the identity of any individual applying for an account; (2) document the information used to verify that person's identity; and (3) screen potential customers against the U.S. Department of the Treasury's Office of Foreign Asset Control's Sanctions List and Specially Designated Nationals List.[156]

The CIP Rules consider different types of accounts and various methods of opening them, as well as different types of identifying information that can be employed.[157] There are several regulations that govern the different types of FIs, including 31 C.F.R. § 1020.220, which is applicable to banks.[158] The CIP Rules are, in turn, passed on from FIs to third-party service providers (including payment processors and mobile wallet/mobile payments providers) as required under the various guidance documents issued by the federal functional financial regulators.[159]

---

[153] *See id.*

[154] *See generally OCC Bulletin 2013-29: Third Party Relationships – Risk Management Guidance*, OFF. COMPTROLLER CURRENCY (Oct. 30, 2013), https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

[155] USA PATRIOT Act of 2001, Pub. L. 107–56 §§ 1–1016, 115 Stat. 272, 317–19; *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 26.

[156] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 26. *See Core Examination Overview and Procedures for Regulatory Requirements and Related Topics: Customer Identification Program-Overview*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_011.htm (last visited Aug. 16, 2017).

[157] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 26. *See* § 326, 115 Stat. at 317–18.

[158] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 26. *See, e.g.*, 31 C.F.R. § 1020.220 (2016).

[159] *Examining the Extensive Regulations of Financial Technologies*, *supra* note

continued . . .

Although not defined as a "financial institution," a payment processor or mobile wallet/mobile payments provider that is either a "provider" or "seller" related to a "prepaid access program" is subject to the U.S. Department of the Treasury's Financial Crimes Enforcement Network's (FinCEN's) Prepaid Access Rule.[160] The Prepaid Access Rule amends the federal money services business (MSB) registration laws (discussed further in Part IV.E below), as was mandated under the Credit Card Accountability Responsibility and Disclosure (CARD) Act of 2009.[161] "'Prepaid access' under the rule covers prepaid devices such as plastic cards, mobile phones, electronic serial numbers, key fobs, and/or other mechanisms that provide a portal to funds that have been paid in advance and are retrievable and transferable."[162] "The final rule:

> • Renames 'stored value' as 'prepaid access,' without narrowing or broadening the meaning of the term, but to more aptly describe the underlying activity.
>
> • Adopts a targeted approach to regulating sellers of prepaid access products, focusing on the sale of prepaid access products whose inherent features or high dollar amounts pose heightened money laundering risks.
>
> • Exempts from the rule prepaid access products of $1,000 or less and pay roll products if they cannot be used internationally, do not permit transfers among users, and cannot be reloaded from a non-depository source.
>
> • Exempts closed loop prepaid access products sold in amounts of $2,000 or less.
>
> • Excludes government funded and pre-tax flexible

120, at 26. *See, e.g.*, *FAQs: Final CIP Rule*, FINCEN 1, 3–4 (Jan. 2004), https://www.fincen.gov/sites/default/files/guidance/finalciprule.pdf; Letter from Bd. of Governors, Maryann Hunter, Acting Dir., Fed. Reserve Sys., to Officer in Charge of Supervision at Each Fed. Reserve Bank, Fed. Reserve Sys. 1 (Mar. 21, 2016), https://www.federalreserve.gov/supervisionreg/srletters/sr1607.pdf.

[160] *See* 31 C.F.R. § 1010.100(t), (ff)(4), (ff)(7) (2016); 31 C.F.R. § 1022.380(a) (2016).

[161] *See* Press Release, FinCEN, FinCEN Issues Prepaid Access Final Rule Balancing the Needs of Law Enforcement and Industry 1–2 (July 26, 2011), https://www.fincen.gov/sites/default/files/news_release/20110726b.pdf. *See also infra* notes 174–79.

[162] Press Release, FinCEN, *supra* note 161, at 2.

> spending for health and dependent care funded prepaid access programs."[163]

Providers of prepaid access are required to register with FinCEN.[164] "Sellers" of prepaid access are retailers of prepaid access devices, which can be physical plastic cards, or the virtual equivalent.[165] Sellers of prepaid access are not required to register with FinCEN—similarly, no MSB operating solely as an agent for another MSB is required to register—sellers of prepaid access "must maintain an anti-money laundering [(AML)] program if the prepaid access product offered is covered" by the Prepaid Access Rule and "can be used *without* a later activation process that includes customer identification, or if a retailer sells prepaid access products . . . providing a portal to funds that exceed $10,000 to any person during any one day."[166]

The definition of "prepaid access" under the Prepaid Access Rule is broad, likely covering prepaid access in the mobile wallet/mobile payments arena.[167] Therefore, to the extent that a mobile wallet/mobile payments provider is a provider of prepaid access, the entity will need to register with FinCEN as a federal MSB and maintain a BSA/AML program.[168] If a mobile wallet/mobile payments provider is a seller of prepaid access, the entity will still need to maintain a BSA/AML program for compliance with the Prepaid Access Rule.[169]

2. "Know Your Customer's Customer" Issues

Over the past several years, various federal agencies have used their review and examination power to recommend that FIs take a very close look at categories of customers or lines of business or industry that are deemed risky or undesirable from a safety and soundness perspective.[170] This regulatory risk is similar to the regulatory risk faced by processors under BSA/AML laws, under which FIs are

---

[163] *Id.*
[164] *Id.*
[165] *See id.*
[166] *Id.* (emphasis added) (alteration in original).
[167] *See id.*
[168] *See id.*
[169] *See id.*
[170] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 25. *See, e.g.*, *BSA/AML Risk Assessment- Overview*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_005.htm (last visited Aug. 16, 2017).

required to evaluate a processor's merchant customer on-boarding and monitoring programs.[171] These are meant "to detect money laundering and terrorist financing, and is referred to generally as Know-Your-Customer's-Customer (KYCC) risk.".[172] For a processor or a mobile wallet/mobile payments provider that is processing payments for other third parties, such nested third-party processing arrangements may be examined by regulators in evaluating the processor or mobile wallet/mobile payments provider as a third-party service provider to an FI, or merely as an FI customer.[173] The areas of focus by regulators, regarding risk, are constantly evolving, but monitoring news developments and interactions with the entity's FI may help the processor or mobile wallet/mobile payments provider stay on top of emerging risky processing areas.[174]

E. FinCEN MSB Registration

Depending upon the services provided and the flow of funds in a mobile wallet/mobile payments transaction, a mobile wallet/mobile payments provider's activity may fall within the definition of "money transmission" at the federal level.[175] While a "payment processor" may be eligible for an exclusion from the requirements to register with FinCEN as an MSB, the parameters of this exclusion require careful evaluation in each case.[176]

In addition, the definition of money transmission and exclusions

---

[171] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 25.

[172] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 25–26. *See* Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29398, 29398–99 (May 11, 2016) (to be codified at 31 C.F.R. pt. 1010, 1020, 1023); Dan Ryan, *FinCEN: Know Your Customer Requirements*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (Feb. 7, 2016), https://corpgov.law.harvard.edu/2016/02/07/fincen-know-your-customer-requirements/.

[173] *See Payment Processor Relationships: Revised Guide*, FED. DEPOSIT INS. CORP. 1, 1–2 (Rev. 2014), https://www.fdic.gov/news/news/financial/2012/fil12003.pdf.

[174] *See generally id.* (discussing third-party processing risks).

[175] *See FinCEN Issues Guidance on Application of Money Transmission Definitions and Exemptions to Certain Business Models*, SIDLEY AUSTIN (May 1, 2014), https://www.sidley.com/en/insights/newsupdates/2014/05/fincen-issues-guidance-on-application-of-money-transmission-definitions-and-exemptions-to-certain-business-models.

[176] *See, e.g.*, *Determination of Money Services Business Status and Obligations Under the Funds Transfer Recordkeeping Rule, and Request for Regulatory Relief*, FINCEN (Nov. 20, 2009), https://www.fincen.gov/sites/default/files/administrative_ruling/fin-2009-r004.pdf.

from MSB registration at the federal level is completely separate and apart from state money transmission licensing regimes.[177] Mobile wallet/mobile payments providers sometimes will mistakenly look only to the federal MSB regulations and not understand that there are still state money transmission laws that apply (as discussed below).[178]

In some instances, a mobile wallet/mobile payments provider may mistakenly believe that registering as a federal MSB takes care of registration as a licensed money transmitter with individual states—this is absolutely not the case, and an entity must comply with both the federal MSB registration and reporting regime as well as the state-level money transmission licensing requirements.[179] Finally, just because an entity determines that it falls within the "processor exemption" of the federal MSB registration requirements, mobile wallet/mobile payments providers should be aware that the presence of a state money transmission law equivalent of a processor exemption must be analyzed on a state-by-state basis, and not every state provides such an exemption from licensing.[180]

F. Unlawful Internet Gambling Enforcement Act

The Unlawful Internet Gambling Enforcement Act (UIGEA) "prohibits gambling businesses from knowingly accepting payment (e.g., credit, electronic fund transfers, check or draft and proceeds from any form of a financial transaction) in connection with the participation of another person in a bet or wager that involves the use of the internet and that is unlawful under any federal or state law in the Act."[181] The "Internet" under this statute is not limited to desktop computer access, but also includes transactions conducted online via mobile devices and mobile phones.[182] Regulations promulgated pursuant to UIGEA further require that "certain participants in

[177] *See* Kelsey L. Penrose, Notes & Comments, *Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws*, 18 N.C. BANKING INST. 529, 545 (2014).

[178] *See infra* notes 187–200 and accompanying text.

[179] *See* Penrose, *supra* note 177.

[180] *See generally* Scott Talbot, *Opinion: States Have Potential to Transform the Regulatory Landscape for Payments*, PAYMENT FACILITATOR (Jan. 19, 2017), http://paymentfacilitator.com/compliance/opinion-states-have-potential-to-transform-the-regulatory-landscape-for-payments/ (stating that in December 2015, Washington State issued an interpretive statement that merchant processing was included as money transmission under the state's Act).

[181] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 31. 31 U.S.C. § 5363 (2012).

[182] *See* 31 U.S.C. § 5362(5) (2006) ("The term 'Internet' means the international computer network of inter- operable packet switched data networks.").

payment systems that could be used for unlawful Internet gambling to have policies and procedures reasonably designed to identify and block or otherwise prevent or prohibit the processing of restricted transactions."[183]

"Participant" is defined as "an operator of a designated payment system, a financial transaction provider that is a member of, or has contracted for financial transaction services with, or is otherwise participating in, a designated payment system, or a third-party processor."[184] "Participants" can include processors or mobile wallet/mobile payments providers.[185] Participants must "establish and implement written policies and procedures reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions," unless, they are subject to certain narrow exceptions.[186] Complying with UIGEA may be problematic for some types of mobile wallet/mobile payments services, and P2P payments may present particular compliance challenges.[187] Nonetheless, given the broad definition of a "participant" under UIGEA, mobile wallet/mobile payments providers should review applicability of this law to their activities and establish a compliance program if needed.

G. State Money Transmitter Laws

One area of surprise and consternation for fintech companies seeking to launch an innovative payment method is state money transmission laws and licensing requirements. These are separate and apart from the federal money services business registration requirements discussed in section IV.E. above.[188] Mobile wallet/mobile payments providers should understand that compliance

[183] *Unlawful Internet Gambling Enforcement Act of 2006 Overview: Attachment A*, FDIC 1, 1 https://www.fdic.gov/news/news/financial/2010/fil10035a.pdf; *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 31–32. *See* 31 U.S.C. § 5364 (2006); *see, e.g.*, 31 C.F.R. § 132.5 (2017).

[184] 31 C.F.R. § 132.2(w) (2009); *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 32.

[185] *See* § 132.2(w); 31 C.F.R. § 132.3 (2009); *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 32.

[186] § 132.5(a); *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 32.

[187] *See generally* Kevin Woodward, *Acquiring: Doubling Down on Gambling and Payments*, DIGITAL TRANSACTIONS (May 1, 2014), http://www.digitaltransactions.net/news/story/Acquiring_-Doubling-Down-on-Gambling-And-Payments (discussing some challenges that mobile wallet payments services could face).

[188] *See supra* notes 174–79 and accompanying text.

with state money transmission laws may also be required.[189]

Consumers are protected from the financial losses associated with conventional money transfer businesses under certain state laws. Western Union is an example of these money transfer businesses because Western Union is an entity conducting money transmission (e.g. accepting money on behalf of Party A to transmit to Part B) and is not otherwise regulated by federal or state financial institution regulators.[190] "Under the conventional money transmission model, the money transfer entity provides a service on behalf of the customer."[191] Essentially, the customer is paying the entity to be a type of intermediary authority between the transferring customer and the desired recipient, who is usually in a different physical location.[192] Due to these heavy consumer-oriented laws, money transmission entities are required to follow detailed licensing and compliance requirements that the states have issued.[193]

> The license application process often includes the payment of a fee and an investigation into the applicant's character, financial situation, and business background. Compliance requirements typically include, for example, obligations to meet minimum net worth requirements, post a surety bond or other security, and submit financial reports. Failure to comply with these requirements can result in criminal and civil penalties.[194]

"[T]hese burdens on the entities regulated by money transmitter laws can be 'onerous and costly,' especially where the money transfer business seeks to operate in multiple states."[195] Moreover, there are certain states who have included provisions in their money transmission statutes that would define money transmission activities to cover almost every type of commercial activity where money is transferred between individuals in different locations (see, e.g.,

---

[189] *See* Penrose, *supra* note 177.

[190] *See* Wistar Wilson, *A Call to Clarify the Regulatory Scope of Money Transmitter Laws*, REG. REV. (June 19, 2013), https://www.theregreview.org/2013/06/19/a-call-to-clarify-the-regulatory-scope-of-money-transmitter-laws/; Kevin V. Tu, *Regulating the New Cashless World*, 65 ALA. L. REV. 77, 94 (2013).

[191] Wilson, *supra* note 190.

[192] *Id.*

[193] *Id.*

[194] *Id.*

[195] *Id.* (alteration in original).

Maryland's money transmission statute).[196] Thus, Internet and mobile payment systems might be caught within these laws.[197]

State regulators are currently taking a variety of positions with regard to whether their particular state money transmission laws apply to payment processors or mobile wallet/mobile payments providers.[198] These state laws often apply on top of federal rules.[199] Therefore, it may be difficult for mobile wallet/mobile payments providers' compliance personnel to adhere to these often inconsistent, and sometimes conflicting, requirements.[200] Companies such as mobile wallet/mobile payments providers can run into challenges with regard to state money transmission licensing depending on the flow of funds in the payment transaction, and whether the mobile wallet/mobile payments provider takes legal possession and control of the funds (even for an instant).[201]

Mobile wallet/mobile payments providers that choose to launch their products and services to the U.S. public writ large via the Internet or mobile devices are essentially offering services to consumers in all fifty states (plus the District of Columbia and U.S. territories).[202] Therefore, launching nationwide requires review of the potential application of money transmission laws in all fifty states (plus the District of Columbia and U.S. territories).[203] Because transmitting money without a license carries potential criminal penalties, this is a very important area for mobile wallet/mobile payments providers to review and ensure compliance.[204]

---

[196] *See* Wilson, *supra* note 190.

[197] *Id.*

[198] *See Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 26–27. *See, e.g.*, Benjamin Lo, *Fatal Fragments: The Effect of Money Transmission Regulation on Payments Innovation*, 18 YALE J.L. & TECH. 111, 132–33 (2016) (identifying California as one of the states that included all domestic money transmissions in its statute, and FaceCash, a mobile wallet, had difficulty applying for a license).

[199] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 27.

[200] *Id. See* Peter Luce, *State Virtual Currency Regulatory Heat Map*, LEXOLOGY (Dec. 19, 2014), https://www.lexology.com/library/detail.aspx?g=b40d933e-f686-4042-8913-2c5bdfdf465c.

[201] *See generally FinCEN Issues Guidance on Application of Money Transmission Definitions and Exemptions to Certain Business Models*, *supra* note 164 (discussing flow of funds and possession in the context of three requests to FinCEN regarding MSB and BSA regulations).

[202] *See, e.g.*, Mailee Garcia, *Walgreens First to Launch Loyalty Program Integration with Apple Pay*, BUS. WIRE (Nov. 5, 2015, 8:00 AM), http://www.businesswire.com/news/home/20151105005216/en/.

[203] *See* Tu, *supra* note 190, at 92.

[204] *See* Wilson, *supra* note 190.

H. State Unclaimed Property Laws and Escheatment Requirements

Another area of legal compliance that mobile wallet/mobile payments providers can sometimes overlook involves state unclaimed property laws and escheatment requirements. Unclaimed property laws vary state-by-state, but generally require the holder of any tangible or intangible property that is legally owned by another individual to "escheat" or "turn over" that property to the state comptroller, treasurer, or other designated agency in the event that the owner of the property cannot be contacted or located after the statutory abandonment period has expired.[205]

Mobile wallet/mobile payments providers that may also be issuers of closed-loop prepaid access accounts are required under the Credit Card Accountability Responsibility and Disclosure Act (CARD Act) to provide certain gift certificate, store gift cards, and general-use prepaid card account holders with the right to access funds for a period of five years from the date the gift certificate, store gift card, or general-use prepaid card account was loaded with funds.[206]

The provisions of Regulation E added by the CARD Act generally apply to gift certificates, store gift cards, and general-use prepaid cards; and include cards, codes, or other devices issued in a specified amount, whether or not they are issued as a physical card.[207] Regulations issued under the CARD Act "apply to an account number or bar code that can access underlying funds; a device with a chip or other embedded mechanism that links the device to stored funds, such as a mobile phone or sticker containing a contactless chip; or an electronic promise."[208] An "electronic promise" is "a person's commitment or obligation communicated or stored in electronic form made to a consumer to provide payment for goods or services."[209] A code that is given as a gift and may be redeemed online is an example

[205] *See* Barbara A. Sangiuliano, *Unclaimed Property: An Overlooked Area of Responsibility for Tax Practitioners*, 16 OCT J. MULTISTATE TAX'N & INCENTIVES 20, 22, 33 (2006).

[206] The CARD Act amended the EFTA, and the rules promulgated by the CFPB with regard to the CARD Act were included within Regulation E at 12 C.F.R. § 1005.20. *See* 15 U.S.C. §§ 1693 (2012); *see also* 12 C.F.R. § 1005.20 (2017) (enumerating requirements for gift card and gift certificates).

[207] Rebecca S. Reagan & Aaron M. Thompson, *Credit CARD Act Requirements for Gift Certificates, Store Gift Cards, and General-Use Prepaid Cards*, CONSUMER COMPLIANCE OUTLOOK 1, 4 (2013). *See* § 1005.20.

[208] Reagan & Thompson, *supra* note 207, at 4–5. *See* § 1005.20 app. C at comment 20(a)1.

[209] 12 C.F.R. § 205.20(a)(2) (Supp. I 2010).

of an electronic promise under the CARD Act.[210]

Escheatment, at the state law level, is when funds, that are considered abandoned, are remitted to the proper state.[211] State unclaimed property laws vary widely in terms of how much time must elapse before funds are deemed abandoned, the process to contact an account holder or successor-in-interest, and what lead to a conclusion that an account is considered to be abandoned.[212]

An additional challenge with regard to escheatment requirements is that even though funds underlying a prepaid card must remain accessible for a period of five years after the funds were loaded under the federal CARD Act, state laws can still impose a shorter "abandonment" period.[213] Therefore, for states with an unclaimed property abandonment period of less than five years, the holder of the funds on the prepaid account must remit the property to the state according to the shorter abandonment period.[214] The holder of the funds must then either (1) make the prepaid account holder whole on transactions that occur before the five-year federal "good funds" expiration period and apply for a refund from the particular state for those amounts, or (2) tell the prepaid account holder that the entity has already remitted funds to a particular state under the state's unclaimed property law, and, therefore, the prepaid account holder will need to obtain the unclaimed property from the state agency to which the company remitted the unclaimed property.[215]

I. Network Rules and Card Associations

The credit card networks (Visa, MasterCard, American Express, and Discover), as well as debit card/ATM networks (e.g., New York Currency Exchange (NYCE) and STAR) and NACHA, which operates the ACH network, all operate via a nexus of contract relationships that include lengthy operating rules and requirements for network

[210] Reagan & Thompson, *supra* note 207, at 5. *See* § 1005.20 app. C at comment 20(a)2.

[211] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 27. *See* Anita Ramasastry, *State Escheat Statutes and Possible Treatment of Stored Value, Electronic Currency, and Other New Payment Mechanisms*, 57 BUS. LAW. 475, 475 (2001).

[212] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 119, at 27. *See* Sangiuliano, *supra* note 205, at 22.

[213] *See* Judith E. Rinearson & Margo Hirsch Strahlberg, *Third Circuit Issues Opinion in New Jersey Abandoned Property Litigation*, LEXOLOGY (Jan. 27, 2012), https://www.lexology.com/library/detail.aspx?g=d4cfee42-1a56-47f4-bfa0-b1770c923cb7.

[214] *See id.*

[215] *See id.*

participants.[216] These contracts require compliance with the network operating rules by payment processors, and to the extent that a mobile wallet/mobile payments provider is acting as a processor, they have such "processing" compliance obligations as well.[217] These networks also enforce certain security standards and requirements, such as the Payment Card Industry Data Security Standards (PCI DSS) discussed below.[218]

Over recent years, these various networks have started defining the different roles that third parties play with regard to origination and settlement of transactions into three categories—payment service provider, payment facilitator, and payment aggregator.[219] A "payment service provider" (PSP) is generally a company that provides merchants with individual merchant accounts in order to perform merchant underwriting and payment processing functions.[220] PSPs help merchants get their merchant accounts and facilitate merchant underwriting and transaction processing.[221] An independent sales organization is an example of a PSP.[222] A PSP does not participate in merchant funding, and merchants are funded directly by the acquiring FI in credit/debit card transactions.[223]

There are important differences between a PSP, a "payment facilitator," and a "payment aggregator."[224] For instance, payment

---

[216] *See, e.g.*, *Description: Risk Management Guidance*, OFF. COMPTROLLER CURRENCY (Sept. 1, 2006), https://www.occ.gov/news-issuances/bulletins/2006/bulletin-2006-39.html (stating that banks should contract to monitor performance and make sure they are in compliance with applicable regulations).

[217] *See Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 30–31. *See, e.g.*, *Mastercard Rules*, MASTERCARD (June 1, 2017), https://www.mastercard.us/en-us/about-mastercard/what-we-do/rules.html.

[218] *See PCI DSS Quick Reference Guide*, PCI SECURITY STANDARDS COUNCIL 1, 6 (May 2016), https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf ("The [PCI DSS] apply to all entities that store, process or transmit cardholder data – with requirements for software developers and manufacturers of applications and devices used in those transactions.").

[219] *See Differences Between PSPs, Payment Facilitators, and Aggregators*, MEDIUM (Sept. 4, 2015), https://medium.com/@UniPayGateway/differences-between-psps-payment-facilitators-and-aggregators-c183065e312d#.z93rxjq9w.

[220] *Id.*

[221] *Id.*

[222] *PSPs, Payment Facilitators, and Aggregators*, UNIPAY GATEWAY (Jan. 14, 2016), http://unipaygateway.com/en/unipay-gateway-payment-advice/psps-payment-facilitators-and-aggregators.

[223] *See id.*

[224] *See Differences Between PSPs, Payment Facilitators, and Aggregators*, *supra* note 219.

facilitators are different because they fund merchants directly.[225] Medium and large-size businesses are essentially the sub-merchants of a payment facilitator since they typically receive their own merchant identification (MID).[226] Thus, if an intermediary entity provides funds to a sub-merchant, and uses a different MID for each merchant, it could be classified as a payment facilitator.[227]

Small businesses and individuals, on the other hand, typically do not even receive their own MIDs and most often work with a "payment aggregator" who uses a single MID to process payments for all sub-merchants in its portfolio.[228] PayPal merchant services is a prime example of a payment aggregator model.[229] A payment aggregator performs merchant funding and may use one MID for all sub-merchants it provides services for.[230] The size of sub-merchants serviced distinguishes payment aggregators from payment facilitators.[231] As a "merchant's processing amounts grow, it might face the legally imposed need to have its own MID, or even become an independent merchant."[232]

With regard to ACH transactions, NACHA makes a distinction between "third-party senders" (TPS) and "third-party service providers" (TPSPs) and has different rules and requirements for each type of entity.[233] At the bare minimum, when a third party moves funds on behalf of another through the ACH network, that entity acts as a TPSP under NACHA rules.[234] Under NACHA, this same entity can *also* be deemed to act as a TPS (a particular type of TPSP); however, this is dependent on whether or not the "originator" (a consumer or business initiating the ACH transaction) or the intermediary entity has an "ACH Origination Agreement" directly with the "originating depository financial institution" (ODFI) for the

---

[225] *Id.*

[226] *Id.*

[227] *PSPs, Payment Facilitators, and Aggregators*, *supra* note 222.

[228] *Differences Between PSPs, Payment Facilitators, and Aggregators*, *supra* note 219.

[229] *See* Peter Lucas, *Cover Story: The Rise of Merchant Aggregators*, DIGITAL TRANSACTIONS (Apr. 1, 2013), http://www.digitaltransactions.net/news/story/Cover-Story_The-Rise-of-Merchant-Aggregators.

[230] *PSPs, Payment Facilitators, and Aggregators*, *supra* note 222.

[231] *Id.*

[232] *Id.*

[233] *See ACH Operations Bulletin #2-2014: ACH Transactions Involving Third-Party Senders and Other Payment Intermediaries*, NAT'L AUTOMATED CLEARING HOUSE ASS'N (Dec. 30, 2014), https://www.nacha.org/news/ach-operations-bulletin-2-2014-ach-transactions-involving-third-party-senders-and-other-payment.

[234] *Id.*

origination of ACH transactions.[235] According to NACHA, "if the intermediary has the ACH Origination Agreement with the ODFI, there is no TPS involved in the transaction, and the intermediary entity is only a [TPSP]."[236] However, if the intermediary entity has the ACH Origination Agreement with the ODFI, and has a separate agreement with the end-user of the services, the intermediary entity acts as a TPS.[237] This distinction is important because of different NACHA rules applying to each type of entity, and also because the intermediary's FI will need to know they are a TPS, as many FIs deem ACH activity as riskier than merely being a TPSP.[238]

Mobile wallet/mobile payments providers need to understand what role their products and services will fall into within the network rules and the ACH rules. For example, the distinctions between a payment service provider, payment facilitator, and payment aggregator are important under the network rules because each category of entity may have varying requirements, and pricing for processing services may also vary.[239] In addition, the networks will want some type of representation that a payment aggregator has appropriate licensing, such as federal MSB and state money transmission licensing.[240] In a payment aggregator model, the service provider uses a single MID, takes legal possession and control of the transaction funds, and takes responsibility for getting the transaction funds to the merchant, and thus payment aggregators often trigger federal MSB registration requirements and state money transmission licensing requirements.[241] For ACH transactions, NACHA rules impose different requirements on TPS as opposed to TPSP.[242] In addition, the specific role under the ACH rules that the mobile wallet/mobile payments provider is playing will need to be disclosed to that entity's own FI.[243]

[235] *Id.*
[236] *Id.*
[237] *Id.*
[238] *See id.*
[239] *See supra* notes 219–27 and accompanying text.
[240] *Id.*
[241] *Id.*
[242] *See ACH Operations Bulletin #2-2014*, *supra* note 233.
[243] *See id.*

V. REGULATORY FRAMEWORK GOVERNING PRIVACY/DATA SECURITY

A. Gramm-Leach-Bliley Act

The federal Gramm-Leach-Bliley Act (GLBA)[244] "requires FIs to provide data security, breach notification, and privacy and data sharing protections to consumers."[245] The Federal Trade Commission (FTC), the CFPB, and each federal functional FI regulatory agency (e.g., Federal Deposit Insurance Corporation (FDIC) and the National Credit Union Administration) have all issued slightly different regulations promulgated pursuant to GLBA regarding how "nonpublic personal information" (NPI) gathered about consumers by FIs will be treated (collectively known as the "Privacy Rules").[246]

FIs are generally obligated to provide notice to customers, and potentially other consumers, about their privacy policies and practices under the Privacy Rules.[247] The Privacy Rules also require that FIs describe when a FI may disclose NPI to nonaffiliated third parties.[248] The Privacy Rules also require that the FI provide a way for customers to prevent the disclosure of their NPI, to nonaffiliated third parties, by giving notice that the customer is opting out of disclosure, subject to certain exceptions.[249]

Under the Privacy Rules, payment processors are considered FIs and, to the extent that a mobile wallet/mobile payments provider is carrying out payment processing functions, the provider is also subject to the Privacy Rules.[250] However, payment processors and mobile wallet/mobile payments providers may not be subject to all of the

---

[244] *See* 15 U.S.C. §§ 6801–6809 (2012).

[245] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 10. *See id.*

[246] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 10. *See* 16 C.F.R. pt. 313 (2017); 12 C.F.R. pt. 1016 (2017); 12 C.F.R. pt. 332 (2017); 12 C.F.R. pt. 573 (2017).

[247] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 10. *See, e.g.*, 12 C.F.R. § 573.1(a)(1) (2000).

[248] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 10. *See* 16 C.F.R. § 313.1(a) (2000); 12 C.F.R. § 1016.1(a) (2016); *id.* §§ 332.7, 332.10 (2009); *id.* §§ 573.7, 573.10 (2009).

[249] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 10.

[250] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 10. *See, e.g.*, 12 C.F.R. § 332.3(k)(1) (2000) ("*Financial institution* means any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities . . . .").

Privacy Rules.[251] For example, payment processors do not fall within the required scope of the FTC and CFPB Privacy Rules because consumers do not become customers of payment processors when the consumer does an ATM, point-of-service, Internet or telephone transaction.[252] A continuing relationship between a customer and a FI is sufficient to establish a customer relationship.[253]

Processors and mobile wallet/mobile payments providers are exempt from the customer notice disclosure requirements because NPI transmitted "in connection with a payment transaction is 'necessary to effect, administer or enforce a transaction' requested by a consumer, or in connection with servicing or processing a financial product or service requested or authorized by a consumer."[254]

While under the Privacy Rules, payment processing does not create a customer relationship or require customer notice, companies must be conscious that *if* a processor or mobile wallet/mobile payments provider also undertakes other activities, such as extensions of credit, deposit of funds, or other services, then the company must determine whether those additional services give rise to requirements to comply with the Privacy Rules.[255] In addition, a processor or mobile wallet/mobile payments provider that is partnering with an FI to, for example, place credit or debit card accounts into a particular mobile wallet, may find that it must comply as a matter of contract or agreements with flow through privacy requirements from the issuing FI's Privacy Rules obligations, which affect its third-party vendors or subcontractors (a category into which a mobile wallet/mobile payments partner will most likely fall).[256]

---

[251] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 10.

[252] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 22. *See* 12 C.F.R. § 1016.4(c) (2016); 16 C.F.R. § 313.4(c) (2000).

[253] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 22. *See* § 313.4(c); § 1016.4(c).

[254] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 22 (quoting 16 C.F.R. § 313.14(a)(1) (2000)). *See also* 16 C.F.R. § 313.14(b)(2)(vi)(A) ("In connection with: the authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited, or otherwise paid using a debit, credit or other payment card, check, or account number, or by other payment means.").

[255] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 22–23. *See* 16 C.F.R. § 313.2 (2009); 12 C.F.R. § 1016.3(j)(2) (2016).

[256] *See generally Financial Institution Letters: Guidance for Managing Third-Party Risk*, FED. DEPOSIT INS. CORP. (June 6, 2008), https://www.fdic.gov/news/news/financial/2008/fil08044a.html (stating that contracts with third parties should include handling information in a manner consistent with the institution's privacy policy and applicable statutes and regulations).

1. GLBA Customer Information Security Guidelines

Payment processors and mobile wallet/mobile payments providers may be defined as "financial institutions" or "service providers" (or both) based on the specific services they supply.[257] If the entity falls into either category, the entity is subject to the guidelines, regarding protecting customer NPI, that the FTC and the federal functional banking regulators have created to carry out Sections 501 and 505(b)(2) of GLBA regarding the Customer Information Security Guidelines (the Security Rules).[258]

If subject to the Security Rules, then the processor or mobile wallet/mobile payments provider must "develop, implement, and maintain a comprehensive written information security program" designed to: "(1) insure the security and confidentiality of [NPI]; (2) protect against any anticipated threats or hazards to the security or integrity of such information; and (3) protect against the unauthorized access to or use of [NPI] that could result in substantial harm or inconvenience to any consumer" whose NPI was obtained by an unauthorized individual.[259]

The Security Rules also generally require appropriate due diligence in the selection of service providers and require contractual obligations to implement appropriate measures, which should be drafted to meet security objectives.[260] FIs are required to monitor the service provider's compliance with these contractual obligations, through conducting or reviewing security audits and requiring summaries of test results and other evaluations of the service provider.[261]

Lastly, as part of the written information security program, an entity that is an FI or a service provider must establish a data breach response protocol that includes an incident response team to notify

---

[257] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 23. *See* 16 C.F.R. §§ 314.1–.4 (2000).

[258] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 23. *See* 15 U.S.C. §§ 6801(b), 6805(b)(2) (2012); § 314.1(a).

[259] 16 C.F.R. § 314.3 (alteration in original); *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 23. *See* 12 U.S.C. § 3404 (1979); 12 C.F.R. pt. 364, app. B, § II (2015); *id.* pt. 208, app. D-2, § II (2014); *id.* pt. 30, app. B, § II (2014); *id.* pt. 570, app. B, § II (2006).

[260] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 11. *See, e.g.*, 12 C.F.R. pt. 364, app. B; *id.* pt. 208 app. D-2; *id.* pt. 30 app. B, § III.D; *id.* pt. 570 app. B.

[261] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 11. *See, e.g.*, 12 C.F.R. pt. 364, app. B; *id.* pt. 208 app. D-2; *id.* pt. 30 app. B, § III.D; *id.* pt. 570 app. B.

affected customers and to timely involve law enforcement.[262] An FI must also ensure that its TPSPs providers are taking appropriate measures to secure customer data and respond to data security incidents.[263]

A processor or mobile wallet/mobile payments provider that is partnering with an FI to, for example, place the credit or debit card accounts that the FI issues into a particular mobile wallet will often find that even though it may not be deemed a "financial institution" itself, it will be deemed to be a "service provider" to its partnering FI.[264] As a result, it must comply as a matter of contract or agreement with the service provider data security program summarized above.[265] In addition, FIs will often require what is colloquially referred to as fourth-party due diligence, where service providers subject to GLBA information security requirements must ensure that all of the service provider's vendors and subcontractors follow the requirements that the service provider must meet.[266]

2. FTC Safeguards Rule Under GLBA

Payment processors and mobile wallet/mobile payments providers are encompassed in the broad definition of "an entity that is 'significantly engaged' in providing financial products or services" and are thus FIs that must comply with the FTC's Standards for Safeguarding Customer Information (the Safeguards Rule).[267] The Safeguards Rule mandates that all FIs, that the FTC has jurisdiction over, "to develop and maintain a comprehensive information security program to safeguard 'customer information.'" [268] Customer

[262] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 11. *See, e.g.*, 12 C.F.R. pt. 570, app. B., supp. A.

[263] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 11.

[264] *See, e.g.*, 12 C.F.R. pt. 570, app. B., supp. A.

[265] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 22.

[266] *See generally* Linnea Solem, *Assurance Process to Address Fourth Party & Subcontracting Risks*, SHARED ASSESSMENTS (July 29, 2014), http://sharedassessments.org/2014/07/assurance-processes-address-fourth-party-subcontracting-risks/ (discussing third-party oversight of fourth parties).

[267] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 23. *See* 16 C.F.R. pt. 314 (2017); *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FED. TRADE COMM'N (Apr. 2006), https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

[268] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 11. *See* 16 C.F.R. §§ 314.2, 314.3 (2000).

information is "defined as any record containing [NPI]."[269] FIs subject to the Safeguards Rule "are required to designate an employee to coordinate the information security program, identify foreseeable security risks, design and implement safeguards to control the risk and test and evaluate the program."[270]

Entities subject to the Safeguards Rule are also required to ensure that service providers, who have access to customer NPI, maintain and implement appropriate security measures.[271] A payment processor or mobile wallet/mobile payments provider partnering with a FI to place the credit or debit card accounts that the FI issues, into a particular mobile wallet, will often find that even though it may not be deemed a "financial institution" itself, it may be categorized as a "service provider," due to its partnering FI, and must comply as a matter of contract or agreement with the Safeguards Rule.[272] FIs will also often require fourth-party due diligence where service providers subject to the Safeguards Rule must ensure compliance by their vendors and subcontractors.[273]

B. PCI DSS

The Payment Card Industry Data Security Standards (PCI DSS) are card transaction security standards published by the Payment Card Industry Security Standards Council (PCI SSC).[274] These security standards are designed to ensure that all merchants and processors that process, store, or transmit card information keep such information in a secure environment.[275] The PCI SSC is made up of five major global credit card companies and other "Strategic Members" from the payments industry.[276] The PCI DSS standards are recognized internationally as the governing standards for the payments

[269] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 11.

[270] *Id.* *See* 16 C.F.R. § 314.4 (2000).

[271] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 11. *See* § 314.4(b)(1)–(2).

[272] *See* §§ 314.2(d), 314.4(d)(1)–(2).

[273] *See generally* Solem, *supra* note 266 (discussing fourth-party compliance).

[274] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 31. *See About Us*, PCI SEC. STANDARDS COUNCIL, https://www.pcisecuritystandards.org/about_us/ (last visited Aug. 17, 2017).

[275] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 31; *Maintaining Payment Security*, PCI SECURITY STANDARDS COUNCIL, https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security (last visited Aug. 17, 2017).

[276] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 31; *Maintaining Payment Security*, *supra* note 275.

industry.[277] They are very detailed and are frequently updated by the PCI SSC to address new developments and threats within the card industry.[278] The PCI DSS standards "apply to any organization or merchant, regardless of size or number of transactions, that accepts, transmits or stores any cardholder data."[279] All payment processors must adhere to these standards, and both merchants and payment processors alike must complete either self-assessments (if they are a smaller organization) or be audited by a "Qualified Security Assessor" (QSA) if they have larger transaction volumes.[280]

PCI DSS requires the installation and maintenance of firewalls, system passwords, encryption of cardholder data across open or public networks, use of anti-virus software, employee access restrictions, physical access restrictions, and development of a card information-specific security policy.[281] They also restrict retention of cardholder data.[282] Failure to comply with PCI DSS can result in significant network penalties in the event of a data security breach that compromises cardholder data.[283]

A mobile wallet/mobile payments provider that "accepts, transmits, or stores" cardholder or card data must abide by PCI DSS.[284] In addition, many merchants as well as FI partners with mobile wallet/mobile payments providers that "accept, transmit, or store" cardholder or card data must contractually represent and warrant that they are PCI DSS compliant, which is often confirmed by attestation from a QSA.[285] In addition, FIs will often require fourth-

[277] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 31. *See PCI DSS Quick Reference Guide: Understanding the Payment Card Industry*, PCI SECURITY STANDARDS COUNCIL 1, 5 (Oct. 2010), https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf.

[278] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 31. *See, e.g.*, *PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users*, PCI SECURITY STANDARDS COUNCIL (July 2014), https://www.pcisecuritystandards.org/documents/Mobile_Payment_Acceptance_Security_Guidelines_for_Merchants_v1-1.pdf.

[279] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 31; *PCI FAQ*, PCI COMPLIANCE GUIDE https://www.pcicomplianceguide.org/faq/ (last visited Aug. 17, 2017).

[280] *See Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 31; *PCI DSS Quick Reference Guide, supra* note 277, at 9.

[281] *See PCI DSS Quick Reference Guide, supra* note 277, at 8.

[282] *See id.* at 14.

[283] *See PCI FAQ*, *supra* note 279.

[284] *Id.*

[285] *See* Tim Thomas, *Merchants: Know Your Service Providers!*, COMPLIANCEGUIDE.ORG (Aug. 7, 2014), https://www.pcicomplianceguide.org/merchants-know-your-service-providers/; *PCI*

continued . . .

party due diligence, by vendors and subcontractors, concerning PCI DSS compliance.[286]

C. State Data Privacy and Data Security Laws

Almost every state, and even most U.S. territories, has enacted some form of data breach notification law.[287] All of those laws classify financial account or card account information as "personal information."[288] A data security breach incident will thus trigger compliance obligations with both federal law and also state data breach notification laws, which may apply based upon the state of residence of the individual whose personal information (including card or financial account data) was compromised.[289]

In addition, in 2007, Minnesota became the first state to specifically require compliance with PCI DSS for card transactions.[290] The Minnesota Plastic Card Security Act[291] prohibits anyone conducting business in Minnesota from storing sensitive information from credit, debit, or stored-value cards for more than forty-eight hours after the transaction has been authorized.[292] The act also makes noncompliant entities responsible for FIs' costs related to cancelling and replacing cards compromised in a security breach.[293] As a result, a data security breach of an entity storing "prohibited" cardholder data (e.g., magnetic stripe, card verification value (CVV) codes, etc.) may be required to reimburse banks and other entities for costs associated with reissuing and blocking cards, with enforcement by private lawsuits.[294] Even though the Act is entitled the "Plastic Card Security

DSS Quick Reference Guide, *supra* note 277, 26–27.

[286] *See generally* Solem, *supra* note 266 (discussing third-party oversight of fourth parties).

[287] *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES, (Apr. 12, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[288] *See Data Breach Charts*, BAKERHOSTETLER 1, 2 (July 2017), https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf.

[289] *Id.* at 11–19.

[290] *See* Dimitri Michaud, *A Growing Movement of PCI Compliance*, INSIDE ARM (Feb. 13, 2008, 4:37 AM), https://www.insidearm.com/news/00030715-a-growing-movement-of-pci-compliance/.

[291] MINN. STAT. ANN. § 325E.64 (West 2017). This statute is also known as the Plastic Card Security Act. *See Popular Names of Acts*, OFF. REVISOR STATUTES, https://www.revisor.mn.gov/topics/?type=statute&id=S7685381&year=2016 (last visited Aug. 10, 2017).

[292] § 325E.64 subdiv. 2.

[293] *Id.* at subdiv. 3.

[294] *Id.* at subdiv. 2.

Act," the provisions of the Act apply to virtually stored payment card data as well.[295]

Mobile wallet/mobile payments providers should understand their obligations under applicable data breach and data security notification laws and develop a data incident response plan.[296] Such a plan should include not only what the entity must do when it suffers a data security breach, resulting in the unauthorized access or acquisition of end-user "personal information" (including card or financial account information), but also should cover how the entity must cooperate with business partners, including the merchants it processes for and the FIs issuing the credit, debit, or stored-value cards that are compromised in any data breach incident.

VI. REGULATORY FRAMEWORK GOVERNING GENERAL CONSUMER PROTECTION

A. Unfair, Deceptive, or Abusive Acts and Practices and Unfair and Deceptive Acts and Practices

1. Dodd Frank Act

Title X of the Dodd-Frank Act, like the FTC Act discussed below, "prohibits covered persons and service providers from engaging in unfair, deceptive, or abusive acts or practices [UDAAP]".[297] It further prohibits any person to "knowingly or recklessly provide substantial assistance to a covered person or service provider" that is engaging in UDAAP.[298] While the CFPB has not clearly laid out rules and standards to advise covered persons and service providers what constitutes a UDAAP, it has defined parameters by publicizing its enforcement actions.[299] A number of potentially abusive, deceptive, or

[295] *See id.*

[296] *See* EXPERIAN, DATA BREACH RESPONSE PLAN 1, 2 (2013–14 ed.), https://www.experian.com/assets/data-breach/brochures/response-guide.pdf.

[297] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 13. *See* 12 U.S.C. § 5536(a)(1)(B) (2012).

[298] § 5536(a)(3); *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 13.

[299] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 13. CFPB Director Richard Cordray announced the precedential value of seeking to glean guidance from previous consent orders, saying that "it would be 'compliance malpractice' for executives not to take careful bearings from the contents of these orders about how to comply with the law and treat consumers fairly." Richard Cordray, Dir., Consumer Fin. Prot. Bureau, Remarks at the Consumer Bankers Association (Mar. 9, 2016), https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-

continued . . .

unfair practices could lead to a UDAAP violation.[300] The CFPB brought its first UDAAP action against a mobile wallet/mobile payments provider for inadequate data security practices in February of 2016.[301] Similar to FIs, enforcement actions may be brought under the Dodd Frank Act for alleged UDAAP violations.[302] While the CFPB has not specifically issued regulations defining UDAAP for payment processors, it has published *Consumer Protection Principles* for the relevant industry.[303] In a decision from the Northern District of Georgia, the court determined that payment processors were "service providers" within the scope of the Dodd Frank Act.[304]

2. FTC Act

The FTC, through the FTC Act, has been granted broad investigative and enforcement powers.[305] Section 5 is relevant to mobile wallet/mobile payments providers and payment processors.[306] It grants the FTC power to forbid unfair or deceptive trade practices.[307] Mobile wallet/mobile payments providers and payment processors, as FIs, fall within the FTC's jurisdiction, and could therefore have enforcement actions brought against them by the FTC.[308] The FTC lacks the authority to issue a regulation that would define unfair or deceptive acts and practices (UDAP), however, guidance may be derived from public enforcement actions.[309] Mobile wallet/mobile

director-richard-cordray-at-the-consumer-bankers-association/.

[300] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 13. *See* 12 U.S.C. § 5531(c)–(d) (2012).

[301] *Examining the Extensive Regulations of Financial Technologies*, *supra* note 120, at 13. *See* Dwolla, Inc., CFPB No. 2016-CFPB-0007, 2016 WL 4523122 (Mar. 2, 2016); *CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices*, CONSUMER FIN. PROT. BUREAU (Mar. 2, 2016), https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/.

[302] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 29. *See* 12 U.S.C. § 5481(6), (15)(A)(vii) (2012).

[303] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 29. *See* discussion *infra* Section IV.C.1.b.

[304] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 29. Consumer Fin. Prot. Bureau v. Universal Debt & Payment Solutions, LLC, No. 1:15-CV-00859-RWS, 2015 WL 11439178 at *15–16 (N.D. Ga. Sept. 1, 2015).

[305] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 119, at 29.

[306] *Id.*

[307] *Id.*

[308] *Id.*

[309] *Examining the Extensive Regulation of Financial Technologies*, *supra* note

continued . . .

payments providers' compliance programs should track their business practices, as well as all FTC enforcement actions, to prevent activities or programs that may be deemed to be UDAP.[310]

3. Telephone Consumer Protection Act

The Telephone Consumer Protection Act (TCPA) "restricts telephone solicitations and limits the use of robocalls (made by way of an automatic dialing system), artificial or prerecorded voice messages, SMS text messages, and junk faxes."[311] The TCPA also specifies technical requirements, that apply to fax machines, auto dialers, and voice messaging systems, that includes identifying the entity that is using the device.[312] If an entity uses an auto dialer or prerecorded message, or engages in telemarketing, in order to reach customers, then it falls under the TCPA.[313] The FCC generally implements and enforces the TCPA, however, the Do Not Call rule, a subdivision of the TCPA, is enforced by the FTC.[314] Furthermore, the TCPA imposes restrictions of the time-of-day during which telemarketing calls may be made (between the hours of 8:00 a.m. and 9:00 p.m. local time).[315] It also grants a private right of action to consumers and specifies the procedures for the Do Not Call Registry.[316]

"With respect to voice calls, the TCPA prohibits a caller from initiating any call to a cell phone or wireless number that was autodialed, or initiating a call that includes a prerecorded or artificial voice without an emergency, or the prior express consent of the recipient (current subscriber or customary user)."[317] Calls to a cell

120, at 29. *See* Cary Silverman & Jonathan L. Wilson, *State Attorney General Enforcement of Unfair or Deceptive Acts and Practices Laws: Emerging Concerns and Solutions*, 65 U. KAN. L. REV. 209, 211–12 (2016).

[310] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 29.

[311] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 14. *See* 47 U.S.C. § 227(b) (2015).

[312] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 14. *See* § 227(d).

[313] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 14. *See* § 227(a)–(b).

[314] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 14. *See* 16 C.F.R. §§ 310.2(g), 310.4(b)(iii)(B) (2016); 47 C.F.R. § 64.1200 (2016).

[315] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 14. *See* 47 C.F.R. § 64.1200(a)(1)–(4), (c), (d).

[316] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 14.

[317] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 14. *See* 47 U.S.C. § 227(a)(2), (b)(1)(B); 47 C.F.R. § 64.1200(f)(5).

phone, that are considered telemarking, including telemarketing calls made under an existing business relationship, require the "prior express written consent" of the recipient.[318] Calls including a prerecorded or artificial voice, made to a landline, are forbidden if the consumer has not given prior express written consent, unless the call is not for a commercial purpose or is made for emergency purposes.[319] Calls made for commercial purposes that do not include an advertisement or telemarketing are also exempted from the prior consent requirement.[320] If a business outsources their telemarking or informational calls to a TPSP, then the business could be held vicariously liable for violations of the TCPA made by a TPSP.[321] This is based off of federal common law agency principles.[322]

With regard to mobile wallet/mobile payments providers, the most relevant aspect of TCPA compliance involves SMS text messaging that the provider may use as part of their service. In general, if the SMS text message is used in conjunction with providing the mobile wallet/mobile payments good or service, such as payment transaction confirmation or alerts, then prior express written consent is not required.[323] However, if the SMS text message includes marketing messages, including marketing for the company's own products and services, then prior written express consent is needed.[324] Prior FTC enforcement actions have also clarified that "prior express written consent" does not occur when such consent is buried in the general terms of use, and that such consent must be obtained in a separate clear and conspicuous manner (such as a separate pop-up box in a mobile app) and cannot be structured as an opt-out consent.[325]

---

[318] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 14. *See* 47 C.F.R. § 64.1200(a)(1)–(a)(2).

[319] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 14. *See* § 64.1200(a)(3).

[320] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 14.

[321] *Id* at 14–15. *See In re* Joint Petition Filed by DISH Network, 28 FCC Rcd. 6574 (2013).

[322] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 15.

[323] *See In re* Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, 30 FCC Rcd. 7961 (2015).

[324] *See id.* at 7968.

[325] *See, e.g.*, Press Release, Fed. Commc'ns Comm'n, FCC Cites First National Bank and Lyft for Telemarketing Violations (Sept. 11, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-335223A1.pdf.

4. Telemarketer Sales (Do Not Call) Rule

The FTC's Telemarketer Sales Rule (TSR) created the National Do Not Call Registry.[326] It allows consumers to enter their phone numbers in order to reduce the number of telephone solicitations they get.[327] "The law requires telemarketers to search the registry every 31 days and avoid calling any phone number on the registry."[328] "A telemarketer who disregards the National Do Not Call Registry could be fined up to $40,000 for each call."[329] Further, the TSR prohibits "credit card laundering," which it defines as "to present or deposit into, or cause another to present or deposit into, the credit card system for payment, a credit card sales draft generated by a telemarketing transaction that is not the result of a telemarketing credit card transaction between the cardholder and the merchant."[330]

The TSR has direct application to consumer-facing businesses.[331] The FTC has begun to use the TSR to impose liability on payment processors who have provided processing services to a telemarketer that has violated the TSR. [332] The FTC imposes liability by alleging that the payment processor has provided "substantial assistance" to the telemarketer violating the TSR. [333] Thus, mobile wallet/mobile payments providers who are processing transactions for third parties should create and maintain payment customer "due diligence" to avoid processing payments for someone who may be accused of

[326] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 15.

[327] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 15. *See Q&A for Telemarketers & Sellers About DNC Provisions in TSR*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/qa-telemarketers-sellers-about-dnc-provisions-tsr (last visited Aug. 13, 2017).

[328] *The Telemarketing Sales Rule*, FTC (Aug. 2016), https://www.consumer.ftc.gov/articles/0198-telemarketing-sales-rule; *id. See* 16 C.F.R. § 310.4(b)(1)(iii)(B), (b)(3)(iv) (2016).

[329] *The Telemarking Sales Rule*, *supra* note 328.

[330] 16 C.F.R. § 310.3(c)(1) (2015); *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 15.

[331] *See Q&A for Telemarketers & Sellers About DNC Provisions in TSR*, *supra* note 327 (stating that TSR provisions cover plans to sell goods or services to consumers through interstate phone calls).

[332] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 29. *See, e.g.*, Stipulated Order for Permanent Injunction & Monetary Judgment, at 2, 8–9, Fed. Trade Comm'n v. Capital Payments, LLC, No. 16-CV-00526, (E.D.N.Y. Feb. 3, 2016), https://www.ftc.gov/system/files/documents/cases/160211bluefinorder.pdf.

[333] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 29.

contravening the TSR.[334]

5. Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA),[335] modified by the Fair and Accurate Credit Transactions Act (FACTA), [336] "regulates consumer reporting agencies, users of consumer reports, and furnishers of consumer information to consumer reporting agencies."[337]

Of particular note to mobile payments providers, the FCRA also has a receipt "truncation" requirement.[338] The truncation requirement also states that no person, who accepts debit or credit cards, may print more than the last five digits of the debit or credit card number on a receipt given at the point of sale or transaction.[339] It also requires that the expiration date of the card not be printed on the receipt.[340] Mobile wallet/mobile payments providers must ensure that the receipt truncation requirements are built into their payment transaction functionality whether there will be printed receipts at the point of sale, e-mail receipts, or in-app receipts stored within the mobile wallet/mobile payments app.[341]

6. Electronic Signatures in Global and National Commerce Act/State Uniform Electronic Transactions Act

The Electronic Signatures in Global and National Commerce (E-SIGN) Act[342] gives electronic documents and electronic signatures the ability to have the same legal effect as paper documents and wet signatures, and was created in order to facilitate electronic agreements and disclosures. [343] After getting the appropriate agreement and

[334] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 29.

[335] 15 U.S.C. §§ 1681–1681x (2012).

[336] Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952.

[337] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 16. *See* 15 U.S.C. §§ 1681b, 1681e.

[338] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 31. *See* 15 U.S.C. § 1681c(g)(1)–(2).

[339] § 1681c(g)(1)–(2); *Examining the Extensive Regulation of Financial Technologies*, *supra* note 119, at 31.

[340] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 31.

[341] *See* 15 U.S.C. § 1681c(g)(1)–(2).

[342] 15 U.S.C. §§ 7001–31 (2000).

[343] *Examining the Extensive Regulation of Financial Technologies*, *supra* note

continued . . .

consent under the E-SIGN Act, FIs and financial services providers may provide most written disclosures electronically, and customers can execute agreements electronically as well.[344] E-SIGN requires a clear and conspicuous statement informing the consumer of his or her rights to a paper copy of records, the right to withdraw E-SIGN consent, and limitations or conditions to the consumer's consent, such as fees for paper copies the consumer requests.[345] Under E-SIGN, companies must also comply with the E-SIGN Act's record retention requirements.[346] In addition to the federal E-SIGN Act, many states have also adopted the model Uniform Electronic Transactions Act (UETA), which in many cases only varies slightly from the federal E-SIGN Act.[347]

For mobile wallet/mobile payments providers, failure to comply with E-SIGN may affect issues such as enforceability of terms of use for the mobile wallet/mobile payments service and the effectiveness of certain required legal disclosures.[348] An agreement such as an "E-SIGN Disclosure and Agreement" should come first in the new customer on-boarding process, before the new customer is presented with any terms of use or disclosures that the entity seeks to conduct electronically.[349] For example, the Square E-SIGN consent that was implemented within the past two years states in part:

> Square, Inc. and its affiliates and third party service providers ("Square") may need to provide you with certain communications, notices, agreements, billing statements, or disclosures in writing ("Communications") regarding our products or services ("Services"). Your agreement to this E-sign Consent

120, at 12. *See* § 7001. E-SIGN does contain exceptions for documents that cannot be executed electronically, and those exceptions are listed at 15 U.S.C. § 7003.

[344] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 12. *See* § 7001(c).

[345] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 12. *See* § 7001(c)(1)(B)(i).

[346] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 13. *See* § 7001(d).

[347] *See* Robert A. Wittie & Jane K. Winn, *Electronic Records and Signatures Under the Federal E-Sign Legislation and the UETA*, 56 BUS. LAW. 293, 299–300 (2000); Brian T. Casey, *Where's the E-Sign? A Primer on Electronic Signature Laws*, L.360 (Aug. 30, 2016, 3:14 PM), https://www.law360.com/articles/833941/where-s-the-e-sign-a-primer-on-electronic-signature-laws.

[348] *See* Budnitz, *supra* note 110, at 13.

[349] *See Electronic Signatures and Customer Consent: Steps to Understanding the E-Sign Process*, CARD SERVS. FOR CREDIT UNIONS (Nov. 1, 2014, 4:10 PM), www.cscunews.net/index/php/166-electronic-signatures-and-customer-consent.

> confirms your ability and consent to receive Communications electronically from Square, its affiliates, and its third party service providers, rather than in paper form, and to the use of electronic signatures in our relationship with you ("Consent"). If you choose not to agree to this Consent or you withdraw your consent, you may be restricted from using the Services.[350]

VII. MISCELLANEOUS REGULATORY REQUIREMENTS

A. FDIC Supervisory Guidance

A non-FI mobile wallet/mobile payments provider is not directly subject to guidance documents from the FDIC or any federal functional regulator.[351] However, the mobile wallet/mobile payments provider is at the very least subject to certain pass-through regulatory requirements by virtue of being the customer of an FI.[352] In addition, if a mobile wallet/mobile payments provider is officially partnered with an FI, then the provider may be subject to additional pass-through regulatory requirements due to the provider's status as a "third-party service provider" to an FI.[353]

Mobile wallet/mobile payments providers should be aware of the FDIC's *Financial Institution Letters* (FILs) and *Supervisory Insights* publications about payment processor relationships with FIs.[354] These

---

[350] *Square E-Sign Consent*, SQUARE, https://squareup.com/legal/sign (last updated Feb. 6, 2017).

[351] *See Mobile Payments: An Evolving Landscape*, *supra* note 87.

[352] *See id.*

[353] *See CFPB Bulletin 2012-03, Service Providers*, CONSUMER FIN. PROTECTION BUREAU (Apr. 13, 2012) http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf; *Third-Party Service Provider Case Studies: ODFI Best Practices to Close the Gap*, NAT'L AUTOMATED CLEARING HOUSE ASS'N 1, 4–5 (2009), http://www.achthirdparty.com/wp-content/uploads/2012/08/thirdpartysenderwhitepaper.pdf.

[354] *See Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 27. *See also FDIC Clarifying Supervisory Approach to Institutions Establishing Account Relationships with Third-Party Payment Processors*, FED. DEPOSIT INS. CORP. (July 28, 2014), https://www.fdic.gov/news/news/financial/2014/fil14041.pdf; *FDIC Supervisory Approach to Payment Processing Relationships with Merchant Customers That Engage in Higher-Risk Activities*, FED. DEPOSIT INS. CORP. https:www.fdic.gov/news/news/financial/2013/fil13043.pdf (last updated July 2014); *Guidance on Payment Processor Relationships*, FED. DEPOSIT INS. CORP., https://www.fdic.gov/news/news/financial/2008/fil08127.pdf (last updated July

continued . . .

publications provide a synopsis of risk areas with regard to third-party relationships that FI regulatory examiners and internal audit teams focus on when reviewing any new mobile wallet/mobile payments customer for banking services, or for partnering as a TPSP.[355] A mobile wallet/mobile payments service provider's compliance team should remain up-to-date on the FDIC and other federal functional regulatory guidance (such as the Federal Reserve System, OCC, National Credit Union Administration, and CFPB) and make sure that the provider's internal policies and procedures are in place to provide satisfactory assurance to the provider's FIs that regulatory guidance is followed by the provider.

B. FFIEC Guidance and Examination

The examination authorities of federal banking regulatory agencies,[356] which make up the FFIEC,[357] include regulation and examination services provided by third parties to insured FIs, such as mobile wallet/mobile payments providers.[358] Because mobile wallet/mobile payments providers must typically contract with an FI to have access to the settlement rails to process payments, providers are considered information technology (IT) service providers subject to examination by the FFIEC member regulatory agencies.[359]

The FFIEC provides guidance to FIs regarding considerations that the institution must take into account in third-party relationships, such as data security, availability and integrity of systems, and compliance.[360] As service providers to FIs, mobile wallet/mobile payments providers must comply with the FFIEC's guidance, are

2014); *see also Supervisory Insights—Summer 2011: Managing Risks in Third-Party Payment Processor Relationships*, FED. DEPOSIT INS. CORP., https://www.fdic.gov/regulations/examinations/supervisory/insights/sisum11/managing.html (last updated July 14, 2014).

[355] *See Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 27.

[356] 12 U.S.C. §§ 1463(a)(1), 1756, 1819(a), 3301 (2012); *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 28.

[357] Financial Institutions Regulatory and Interest Rate Control Act of 1978, Pub. L. No. 95–630, 92 Stat. 3641 (1978) (codified in various provisions of 12 U.S.C.); *Examining the Extensive Regulation of Financial Technologies*, *supra* note 119, at 28.

[358] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 28. *See Retail Payment Systems*, FED. FIN. INSTITUTIONS EXAMINATIONS COUNCIL 1, A-1, E-1 (Apr. 2016), https://ithandbook.ffiec.gov/media/211685/retailpaymentsystems2016.pdf.

[359] *Retail Payment Systems*, *supra* note 358, at 1–2, E-1 to -18.

[360] *See id.* at 46.

subject to examination by all the functional bank regulators (federal and state) and the CFPB, and are also subject to audit by all of the FIs the provider uses and has relationships with.[361]

In order to maintain compliance, as well as deal with audit or examination requests, mobile wallet/mobile payments providers should keep detailed compliance manuals, policies, and procedures, as well as compliance controls and compliance programs.[362] To stay on top of compliance obligations, at a minimum, a chief compliance officer is required, and generally other staff may be required as well, dependent on payment services offered, and the states in which a company is doing business.[363]

VIII. CONCLUSION

There are many creative and innovative companies and developers who seek to launch new and innovative fintech companies in the mobile payments/mobile wallet arena.[364] Many of these companies are startups launched by talented programmers and developers who think "there has to be a better way."[365] However, as this article seeks to demonstrate, there are many existing laws, rules and regulations that apply to many activities within the mobile payments/mobile wallet areas of the fintech space—whether the companies developing these apps know it or not. Companies seeking to launch such products and services are well-advised to understand and seek legal advice on their product or service to determine if, when and how existing laws, rules and regulations apply to activities they are engaging in.

Financial services is one of the three most heavily regulated industries in the U.S. (the others being healthcare and energy), so new entrants must understand they are entering a regulated industry.[366] And the laws, rules and regulations that apply are not only those

---

[361] *See id.* at E-1 to -18.

[362] *Examining the Extensive Regulation of Financial Technologies*, *supra* note 120, at 28.

[363] *Id.*

[364] *See* Sig Ueland, *11 Innovative Mobile Payment Apps*, PRACTICAL ECOMMERCE (May 10, 2015), http://www.practicalecommerce.com/11-Innovative-Mobile-Payment-Apps.

[365] *See* Lori Kozlowski, *Mobile Retail: Making Your Wallet Work for You*, FORBES (Sept. 4, 2013, 12:15 PM), https://www.forbes.com/sites/lorikozlowski/2013/09/04/mobile-retail-making-your-wallet-work-for-you/#23fa1d3759ec.

[366] *See* Kasia Moreno, *Regulatory Environment Has More Impact on Business Than the Economy, Says U.S. CEOs*, FORBES (Aug. 12, 2014, 4:22 PM), https://www.forbes.com/sites/forbesinsights/2014/08/12/regulatory-environment-has-more-impact-on-business-than-the-economy-say-u-s-ceos/#795e78fd684d/.

promulgated and enforced by traditional FI regulators. The TCPA, for example, has regulations promulgated and enforced by the FCC, and the FTC has broad authority with regard to privacy/data security as well as UDAP enforcement.[367] At the same time, traditional regulators are trying to learn about and reach out to new entrants in the fintech space who seek to offer regulated services, and can be valuable resources in educating fintech entrants in the mobile payments/mobile wallet space with regard to how regulators view these emerging forms of products and services.[368] As technology and innovation continues to grow in this area of the fintech economy, the watchword for new entrants into the space is "compliance-by-design" for their financial products and services.

[367] *See Privacy & Data Security Update (2016)*, FED. TRADE COMM'N (Jan. 2017), https://www.ftc.gov/reports/privacy-data-security-update-2016.

[368] *See* Carmen Germaine, *American Regulators Playing FinTech Catch Up*, L.360 (June 15, 2017, 11:08 PM), https://www.law360.com/articles/935250/american-regulators-playing-fintech-catch-up.