UNIVERSITY *of* PENNSYLVANIA
LAW REVIEW

Founded 1852

Formerly
AMERICAN LAW REGISTER

VOL. 166 JANUARY 2018 NO. 2

ARTICLE

PANDORA'S DIGITAL BOX: THE PROMISE AND PERILS OF DIGITAL WALLETS

ADAM J. LEVITIN†

Digital wallets, such as ApplePay and Google Pay, are smart payment devices that can integrate payments with two-way, realtime communications of any type of data. Integration of payments with realtime communications holds out tremendous promise for consumers and merchants alike: the combination, in a single, convenient platform, of search functions, advertising, payment, shipping, customer service, and loyalty programs. Such an integrated retail platform offers consumers a faster and easier way to transact, and offers brick-and-mortar retailers an eCommerce-type

† Professor of Law, Georgetown University Law Center. This Article is based on a study I was commissioned to write by the Merchant Advisory Group, a retail industry trade association focused on payments issues. The Merchant Advisory Group facilitated interviews with the payments and treasury teams of a number of its merchant members on a no-attribution basis, but did not exercise any control over the content or conclusions of the study or this Article. The views presented in this Article do not necessarily represent the positions of the Merchants' Advisory Group or its members. Thank you to Steve Salop and Chris Hoofnagle for helpful comments and to Kimberly Chan for research assistance.

ability to identify, attract, and retain customers. At the same time, however, digital wallets present materially different risks for both consumers and merchants than traditional plastic card payments precisely because of their smart nature.

For consumers, digital wallets can trigger an unfavorable shift in the applicable legal regime governing the transactions, increase fraud risk, create confusion regarding error resolution, expose consumers to non–FDIC-insured accounts, and substantially erode transactional privacy. These risks are often not salient to consumers, who thus cannot distinguish between different digital wallets on the basis of risk. Consumers' inability to protect against these risks points to a need for regulatory intervention by the Consumer Financial Protection Bureau to ensure minimum standards for digital wallets.

For merchants, digital wallets can divest valuable customer information used for antifraud, advertising, loyalty, and customer service purposes. Digital wallets can also facilitate poaching of customers by competitors, impair merchants' customer relationship management, deprive merchants of influence over consumers' payment choice and routing, increase fraud risk, subject merchants to patent infringement liability, and ultimately increase the costs of accepting payments. Merchants are constrained in their ability to refuse or condition payments from digital wallets based on the risks presented because of merchant rules promulgated by credit card networks. These rules raise antitrust concerns because they foreclose entry to those digital wallets that offer merchants the most attractive valuation proposition: wallets that do not use the credit card networks for payments.

INTRODUCTION

Digital wallets are poised to transform the world of consumer payments and commerce. Digital wallets are computer software applications that store and transmit payment authorization data for one or more credit or deposit accounts. After a consumer loads her payment account data into a digital wallet, the digital wallet functions as a payment device for the selected account, transmitting the data to merchants to authorize payment. By storing payment authorization data, digital wallets function analogously to physical wallets that contain multiple payment cards used to transmit payment authorization data.

Digital wallets differ from traditional plastic cards in that they are (potentially) smart wallets. Traditional payment cards are "dumb" devices that are capable of doing a single thing and nothing more: transmitting payment

authorization data to a merchant. In contrast, a digital wallet can provide two-way communication between a consumer and a merchant. That communication need not be limited to payment authorization data, but could include virtually any type of data. For example, a digital wallet can be used to transmit realtime geolocation data, coupons, and loyalty program information about the consumer to the merchant. It can also be used to transmit advertising, sales offers, shipping information, and receipts from the merchant to the consumer in real time. This means that a digital wallet can potentially integrate payments into a comprehensive digital retail services suite of advertising, search, payment, customer service, and loyalty program features.

Despite the basic functional similarity to traditional plastic payment cards, digital wallets can present materially different risks and costs for consumers and merchants. Critically, these risks and costs vary among digital wallets. Digital wallets involve a much broader range of form factors, technologies, and business models than traditional plastic cards, and the cost–benefit proposition of making or accepting digital wallet payments varies by product.

For consumers, digital wallets can unfavorably shift the legal regime that governs the transactions, expose individual consumers to additional fraud risk, sow confusion regarding error resolution, expose consumers to non–FDIC-insured accounts, and substantially erode transactional privacy. For merchants, the risks from digital wallets include losing valuable customer information, poaching of customers by competitors, and impairing customer relationship management, as well as increases in fraud risk, patent infringement liability, and the cost of accepting payments.[1]

Unfortunately, neither consumers nor merchants can effectively protect their interests with respect to digital wallets, albeit for different reasons. Although consumers have a largely unconstrained ability to pick and choose which digital wallet(s) to use, this ability affords little market-based protection for two reasons. First, the types of risks digital wallets pose to consumers are unlikely to be salient in their decisionmaking. Second, even if these risks were salient, consumers lack the ability to distinguish between digital wallets with regard to these risks. Consumers' lack of understanding of the material risks involved with digital wallets and their inability to protect their interests when selecting digital wallets points to the need for regulatory intervention to mandate minimum consumer protections for digital wallets. The Consumer Financial Protection Bureau (CFPB) has authority to undertake such regulation.

Merchants face a different problem. Merchants have only limited ability to refuse or condition acceptance of payments from particular digital wallets. The three major payment card networks—American Express, MasterCard, and Visa (collectively, the Card Networks)—have network rules applicable to merchants

1 Other risks, such as compliance with anti–money laundering laws, are beyond the scope of this Article.

that accept their cards. The Card Networks' rules require merchants to "Honor All Wallets" without discrimination. Specifically, the Honor All Wallets rules require merchants that choose to accept a Card Network's payments using a particular type of communications technology to accept the Card Network's payments without discrimination from all devices that utilize that communications technology. These rules force merchants to take various types of digital wallets if they accept regular credit and debit payments—which is a *sine qua non* of participating in modern retail markets.

For example, a merchant that accepts traditional MasterCard magnetic stripe devices must accept MasterCard payments from all devices using magnetic stripe data, including mobile devices such as SamsungPay that utilize magnetic stripe emulation technology to mimic the electromagnetic field created by a magnetic stripe card. Likewise, if a merchant accepts Visa contactless payments from credit cards with Near Field Communications (NFC) "contactless" chips, the merchant must also accept Visa contactless payments from all mobile devices that use NFC.[2] The merchant could not accept NFC payments only from mobile devices that make payments through lower-cost systems like PIN-debit and automated clearing houses (ACH).[3]

Under the Honor All Wallets rules, then, a merchant must accept payments from all payment devices that utilize a technology if the merchant accepts any payments using that technology. As a result, merchants cannot refuse to accept payments from payment devices that impose greater risks and costs upon them. Merchants cannot price for the risks created by particular payment devices, nor can they contractually reallocate those risks to the digital wallet provider. Indeed, absent direct physical observation, merchants are presently unable to identify what form factor was used to make a payment, so merchants cannot even distinguish which digital wallet is being used.

In sum, the Honor All Wallets rules mean that merchants lose control over what risks they accept and on what terms. When accepting payment

2 NFC is a type of high-frequency radio frequency identification (RFID) communication. RFID usually refers to a combination of a separate "tag" and "reader" that communicate through an antenna, whereas an NFC card functions sometimes as a tag and sometimes as a reader, as illustrated by "tap" transactions between two NFC devices. NFC devices are made to specifications promulgated by the NFC Forum, which certifies devices for compliance with these standards. The NFC Forum's top-level members include MasterCard and Visa. For more on NFC, see generally THOMAS LERNER, MOBILE PAYMENT (2013), and JOHNSON I. AGBINYA, PRINCIPLES OF INDUCTIVE NEAR FIELD COMMUNICATIONS FOR INTERNET OF THINGS (2011).

3 ACH is an electronic payment method for moving funds between accounts at depository institutions. There is no access device for using ACH. Instead, funds are transferred with bank account and routing numbers. Direct deposit and automatic bill pay are two common uses of ACH. For more on ACH, see generally NAT'L CONSUMER LAW CENTER, CONSUMER BANKING AND PAYMENTS LAW § 5.1.5.2 (5th ed. 2013).

from any particular digital wallet, a merchant is forced to open a digital Pandora's Box of an unknown set of risks.

This Article considers the potential legal and business issues digital wallets raise for both consumers and merchants, and proposes a pair of necessary interventions in the digital wallet marketplace. First, it argues the CFPB should issue regulations under its power to regulate "abusive" practices and services to require minimum standards for default payment options, security, deposit insurance coverage, and privacy. Second, it argues the Honor All Wallet rules are likely antitrust violations that inhibit the development of digital wallet technology by making merchants reluctant to accept digital wallets and by making it difficult for the digital wallets with the most attractive value propositions for merchants to gain market share. In particular, the Honor All Wallets rules foreclose entry into the digital wallet market for digital wallets that use lower cost payment systems than the Card Networks—namely PIN-debit and ACH—and thereby help the Card Networks maintain their market power in the face of a technological transition from plastic cards to digital wallets. Ironically, then, the Honor All Wallets rules may well be *inhibiting* rather than *encouraging* adoption of digital wallets because the rules enable bad wallets to preserve market access such that the bad can crowd out the good.

This Article contributes to the consumer protection, antitrust, and payment systems literatures. Consumer protection literature is only just starting to address the tremendous and ongoing technological changes in payments.[4] This Article lays out the rationale and authority for CFPB intervention to require minimum product standards in the digital wallet market.

The payments industry has been beset with antitrust litigation in the United States for the past two decades, focusing on the Card Networks' system for setting interbank fees on payments (which get passed through to merchants and consumers), including various Card Network rules that prohibit merchants from taking actions to steer consumers to cheaper payment methods. This litigation has resulted in two of the largest private settlements in history—a $3 billion class action settlement in 2003[5] and a $7 billion class action settlement in 2013 (which was subsequently thrown out on appeal)[6]—and a pair of Department of Justice

4 *See, e.g.*, Mark Edwin Burge, *Apple Pay, Bitcoin, and Consumers: The ABCs of Future Public Payments Law*, 67 HASTINGS L.J. 1493 (2016); Kevin V. Tu, *Regulating the New Cashless World*, 65 ALA. L. REV. 77 (2013); Mark E. Budnitz, *The Legal Framework of Mobile Payments: Gaps, Ambiguities, and Overlap* (Ga. State Univ. Coll. of Law, Legal Studies Research Paper No. 2016-22, 2016), https://ssrn.com/abstract=2841701 [https://perma.cc/BCA8-4U99]; Niels Vandezande, *Mobile Wallets and Virtual Alternative Currencies Under the EU Legal Framework on Electronic Payments* (Interdisciplinary Ctr. for Law & ICT Working Paper 16/2013, 2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325410 [https://perma.cc/H5VK-KDGL].

5 *In re* Visa Check/Mastermoney Antitrust Litig., 297 F. Supp. 2d 503 (E.D.N.Y. 2003), *aff'd sub nom.* Wal-Mart Stores, Inc. v. Visa U.S.A. Inc., 396 F.3d 96 (2d Cir. 2005).

6 *In re* Payment Card Interchange Fee & Merch. Disc. Antitrust Litig., 986 F. Supp. 2d 207 (E.D.N.Y. 2013), *rev'd*, 827 F.3d 223 (2d Cir. 2016).

suits.[7] The same practices were also targeted by part of the Dodd–Frank Wall Street Reform and Consumer Protection Act of 2010[8] and have been the focus of intense regulatory scrutiny outside the United States.[9]

At issue in much of the litigation and regulatory reforms is the application of antitrust law to so-called "two-sided" markets—markets in which there are two types of "consumers" of a product. In the case of payments, the two types of consumers are merchants and actual consumers. A sizeable scholarly literature has emerged on two-sided markets[10] and on the application of antitrust law to those markets, particularly with reference to payment cards.[11]

---

7 United States v. Visa U.S.A., Inc., 344 F.3d 229 (2d Cir. 2003) (affirming a district court's ruling that MasterCard and Visa's dual exclusivity structure for issuers violated antitrust law); United States v. Am. Express Co., 88 F. Supp. 3d 143 (E.D.N.Y. 2015) (finding American Express's antisteering rules to be antitrust violations), *rev'd & remanded*, 838 F.3d 179 (2d Cir. 2016); *see also* Final Judgment as to Defs. Mastercard Int'l & Visa Inc., United States v. Am. Express Co., 2011 U.S. Dist. LEXIS 87560 (E.D.N.Y. July 20, 2011) (No. CV-10-4496) (detailing terms of a consent decree between the Government, MasterCard, and Visa in a suit brought against American Express, Mastercard, and Visa over antisteering rules).

8 *See* Pub. L. No. 111-203, § 920, 124 Stat. 1376, 2068-74 (codified at 15 U.S.C. § 16930-2 (2012)).

9 *See, e.g.*, Regulation 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions, 2015 O.J. (L 123) 10-11 (capping interchange fees for debit and credit card transactions); Case C-382/12 P, MasterCard v. Comm'n, 2014 Curia ¶ 168, http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=1&part=1&mode=lst&docid=147066&occ=first&dir=&cid=1142943 [https://perma.cc/7CGF-TUHD] (rejecting MasterCard's appeal after the European Commission brought a successful antitrust challenge to MasterCard's cross-border interchange fees); RESERVE BANK OF AUSTL., COMMON BENCHMARK FOR THE SETTING OF CREDIT CARD INTERCHARGE FEES 1 (2005), https://www.rba.gov.au/payments-and-infrastructure/credit-cards/cc-fees-benchmark/pdf/cc-fees-benchmark.pdf [https://perma.cc/B6X4-2LZN] (limiting interchange fees for Australian credit card transactions); *see also* Adam J. Levitin, *Priceless? The Economic Costs of Credit Card Merchant Restraints*, 55 UCLA L. REV. 1321, 1389 n.241 (2008) (noting that Finland, the Netherlands, Portugal, and Sweden ban surcharge restrictions for credit and debit cards, while the U.K. bans surcharge restrictions only for credit cards).

10 *See, e.g.*, Mark Armstrong, *Competition in Two-Sided Markets*, 37 RAND J. ECON. 668 (2006); Bernard Caillaud & Bruno Jullien, *Chicken & Egg: Competition Among Intermediation Service Providers*, 34 RAND J. ECON. 309 (2003); Jean-Charles Rochet & Jean Tirole, *Two-Sided Markets: A Progress Report*, 37 RAND J. ECON. 645 (2006); Roberto Roson, *Two-Sided Markets: A Tentative Survey*, 4 REV. NETWORK ECON. 142 (2005); E. Glen Weyl, *A Price Theory of Multi-Sided Platforms*, 100 AM. ECON. REV. 1642 (2010); Julian Wright, *One-Sided Logic in Two-Sided Markets*, 3 REV. NETWORK ECON. 44 (2004).

11 *See, e.g.*, DAVID S. EVANS, INTERCHANGE FEES (2011); Hélène Bourguignon et al., *Card Surcharges and Cash Discounts: Simple Economics and Regulatory Lessons*, 10 COMPETITION POL'Y INT'L 13 (2014); Dennis W. Carlton & Alan S. Frankel, *The Antitrust Economics of Credit Card Networks*, 63 ANTITRUST L.J. 643 (1995); Sujit Chakravorti, *Theory of Credit Card Networks: A Survey of the Literature*, 2 REV. NETWORK ECON. 50 (2003); Benjamin Edelman & Julian Wright, *Price Coherence and Excessive Intermediation*, 130 Q.J. ECON. 1283 (2015); Adam J. Levitin, *Payment Wars: The Merchant-Bank Struggle for Control of Payment Systems*, 12 STAN. J. L. BUS. & FIN. 425 (2007) [hereinafter Levitin, *Payment Wars*]; Adam J. Levitin, *The Antitrust Super Bowl: America's Payment Systems, No-Surcharge Rules, and the Hidden Costs of Credit*, 3 BERKELEY BUS. L.J. 265 (2005); Levitin, *supra* note 9; Adam J. Levitin, *Priceless? The Social Costs of Credit Card Merchants Restraints*, 45 HARV. J. ON LEGIS. 1 (2008); Jean-Charles Rochet & Jean Tirole, *An Economic Analysis of the Determinants of Interchange Fees in Payment Card Systems*, 2 REV. NETWORK ECON. 69 (2003); Jean-Charles Rochet & Julian Wright, *Credit Card Interchange Fees*, 34 J. BANKING & FIN. 1788 (2010); Marius Schwartz & Daniel R. Vincent, *The No Surcharge Rule and Card User Rebates: Vertical Control by a Payment Network*, 5 REV. NETWORK ECON. 72 (2006); Steven C. Salop

Courts, however, are only just beginning to grapple with the issue.[12] This Article situates the Honor All Wallets rules in this context as representing a new application of the antitrust problems that arose from the related Honor All Cards rules, which require merchants to accept all of a Card Network's plastic cards if the merchant accepts any of the Network's cards.

The Article also contributes to the payment systems literature by serving as a technical guide to digital wallets and their underlying security technologies: Chip (EMV) cards, tokenization, and encryption. The literature on payment systems has not kept pace with technological innovation, and this Article fills an important lacuna. Without an understanding of the technical issues, lawyers cannot identify the legal issues involved with digital wallets.

The Article proceeds as follows: Part I examines the traditional structure and economics of payment transactions and how digital wallets change it. Section II.A examines the benefits and costs of digital wallets to consumers and presents the argument that the CFPB should undertake rulemaking to address digital wallets. Section II.B examines the benefits and costs of digital wallets to merchants and presents the argument that the Honor All Wallets rules are likely an antitrust violation inhibiting entry into the market by digital wallets that use cheaper payment methods, such as PIN-debit and ACH.

I. DIGITAL WALLETS AND MOBILE PAYMENTS

A. *Flows of Funds and Data in Payment Card Transactions*

A traditional card-based payment, whether credit or debit, involves five parties: the consumer, the merchant, the consumer's bank, the merchant's bank, and the payment card network. The consumer's bank is known as the "issuer" because it issues the card to the consumer.[13] The card contains payment authorization data that allows the consumer to access either a line of credit with the issuer (for a credit card) or a demand deposit account (for a debit card). The merchant's bank is known as the "acquirer" because it acquires the payment from the merchant by paying the

& Fiona Scott Morton, *Developing an Administrable MFN Policy*, ANTITRUST MAG., Spring 2013, at 15; Adam J. Levitin, *Cross-Routing: PIN and Signature-Debit Interchangeability Under the Durbin Amendment* (Georgetown Univ. Law Ctr. Bus. Econ. & Regulatory Policy Working Paper Series, Research Paper No. 1681078, 2010), https://www.federalreserve.gov/newsevents/rr-commpublic/levitin_paper_20101124.pdf [https://perma.cc/88DK-9C2G]; Alan O. Sykes, *Antitrust Issues in Two-Sided Network Markets: Lessons from* In Re Payment Card Interchange Fee and Merchant Discount Antitrust Litigation (N.Y.U. Law & Econ. Research Paper Series, Working Paper No. 14-45, 2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2530657&rec=1&srcabs=2681304&alg=1&pos=3 [https://perma.cc/4BPQ-Y3M3].

12 To date, only one appellate decision has directly addressed this issue: *United States v. Am. Express Co.*, 838 F.3d 179 (2d Cir. 2016) (holding the Government did not meet its burden to prove an antitrust violation), *cert. granted*, No. 16-454, 2017 WL 2444673 (Oct. 16, 2017) .

13 In the American Express system, the payment card network also serves as the acquirer, and often as the issuer, although American Express has allowed third-party issuance since 2005.

merchant an amount discounted from the face amount of the transaction. This discount is known as the "merchant discount fee." The merchant discount fee is individually negotiated between acquirers and merchants. The acquirer will then present the transaction for payment to the issuer through the payment card network, which functions as a clearinghouse between acquirers and issuers.[14]

The payment card network promulgates the rules for the involved parties. Formally, the payment card network has contractual relationships with only the acquirer and issuer banks. Merchants find themselves subject to card network rules by virtue of the rules' incorporation in merchants' contracts with their acquirer banks.

The payment card networks charge acquirers and issuers various network fees for their services. The payment card networks also collect an interchange fee from the acquirer that is remitted to the issuer bank in the form of an additional discount from the transaction's face value. Interchange fees are formally an interbank fee paid by acquirers to issuers, but they are not individually negotiated between acquirers and issuers. Instead, interchange fees are determined by a fee schedule set by the payment card network. The interchange fee varies by merchant type and transaction volume, as well as by the features of the consumer's payment card (credit, debit, level of rewards on the card, etc.), rather than by the banks' risk characteristics. Interchange fees are typically an *ad valorum* fee plus a flat fee, although for debit card transactions the interchange fee is sometimes a capped flat fee.

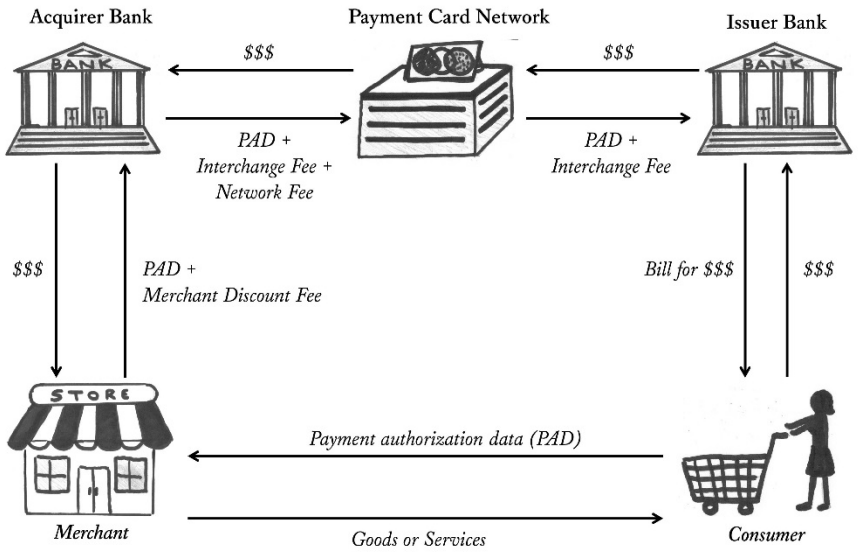
Because acquirers are faced with an interchange fee on every transaction, acquirers set the merchant discount fee above the interchange fee plus network fees; the interchange fee plus the network fees are a floor for the merchant discount fee. Indeed, some acquirers offer pricing that is explicitly "interchange plus," meaning that there is direct pass-through to the merchant of the interchange fee plus an additional margin for the acquirer. Consequently, merchants have the ability to negotiate only the acquirer's merchant discount fee over and above the interchange fee.

Thus in a traditional payment card transaction the cardholder transmits her payment authorization data, including her primary account number (PAN) to the merchant, which relays the information to the acquirer bank and thence through the Card Network to the issuer for authorization. If the transaction is authorized, the issuer will remit funds to the network, which will send them on to the acquirer bank and thence to the merchant. At each step of the way,

14 Acquirers will frequently outsource many of their functions to third-party payment processors and independent service organizations (ISO). *See* Ramon P. DeGennaro, *Merchant Acquirers and Payment Card Processors: A Look Inside the Black Box*, 91 FED. RES. BANK ATLANTA ECON. REV. 27, 31 (2006). Although processors and ISOs play a major practical role in card payments, they are functionally acting as agents between the acquirer and merchant, rather than as a foundational part of the card payment system.

however, the remitted funds are reduced by the associated offsetting fee: the interchange fee, the network fees, and the merchant discount fee.[15] Figure 1 illustrates the flow of data and money in a payment card network.

Figure 1: Payment Card Transaction Overview



The value received by the merchant in a traditional payment card transaction is not limited to the transaction amount minus the merchant discount fee. An important part of the value to a merchant of a payment card transaction comes in the form of information about the consumer. Payment

15 The technical details of the data transmission process are slightly different for credit cards and most signature-authorized debit cards than for PIN-authorized debit cards. Credit cards and most signature-debit cards use two separate messages among the merchant, acquirer, payment network, and issuer for authorization of the transaction, clearing, and settlement of the funds into the merchant's account at the acquirer. One message contains the authorization request, while a second message will contain the clearing and settlement communications. Authorization is separated from clearing and settlement because clearing and settlement are not conducted separately in real time for individual transactions, but rather processed periodically in batches. *See generally* NAT'L CONSUMER LAW CENTER, *supra* note 3, § 5.1.5.2.

PIN-debit cards, in contrast, use a single message for authorization, clearing, and settlement. There is, nonetheless, only a single settlement, which occurs on an individual transaction basis in near-realtime, just like an ATM withdrawal. Even with single messaging, however, settlement is still done on a periodic, aggregate basis, rather than by individual transaction. For a detailed overview of MasterCard's clearing and settlement functions, which are emblematic of those of other card networks, see generally Susan Herbst-Murphy, *Clearing and Settlement of Interbank Card Transactions: A MasterCard Tutorial for Federal Reserve Payments Analysts*, FED. RESERVE BANK OF PHILA. (Oct. 2013), https://www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2013/D-2013-October-Clearing-Settlement.pdf [https://perma.cc/94S5-R4HW].

card transactions are much more informationally rich than cash transactions because they associate a particular, identifiable consumer with a transaction.

In a traditional payment card transaction, the cardholder's PAN is fully visible to the merchant. The PAN is a customer-specific identifier that is a source of significant value to the merchant. Merchants can mine PAN data to correlate past purchases made using the same PAN and use this information for fraud detection, advertising, customer loyalty programs, and to facilitate returns and exchanges. The ability to track a customer's purchase history by PAN means that merchants can set up fraud tripwires for purchases made in unusual locations, at unusual times, for unusual amounts, or even for unusual items. At the same time, the ability to track purchase history by PAN enables merchants to target advertising and loyalty programs at particular consumers and for particular merchandise. For example, a merchant that notices a pattern of purchases of baby-related items might choose to send the consumer advertisements and coupons that focus on baby products over the next year, because baby-related purchases by parents are unlikely to occur only once.

The ability to track PANs also facilitates customer relationship management. For example, a husband and wife who share a credit card account will each have a card with the same PAN. An erroneous purchase by the hapless husband can easily be returned by the wife if she has a receipt because her card's PAN will match that of the card used by her husband to make the purchase. Thus the ability to see and track a consumer's PAN is valuable for merchants in a range of applications.

B. *Digital Wallets*

Digital wallets build on the traditional payment card network structure. Though digital wallets do not change the fundamental transaction, they instead may change the method and nature of the data communicated between consumers and merchants.

A digital wallet is a computer software application that stores and transmits payment authorization data for one or more credit or deposit accounts. Once a consumer loads her payment account data into a digital wallet, the digital wallet can then be used as a payment device for that account, transmitting the data to merchants to authorize payment.

1. Types of Digital Wallets

The term "digital wallet" encompasses a broad range of products. These products vary in four dimensions: acceptance, funding, pass-through versus staged

status, and form factor.[16] Acceptance refers to where the wallet can be used to make payments. Some wallets are "general purpose wallets" that can be used for payments at any merchant, while others are "business wallets" that can be used only at a single merchant or group of associated merchants, much like a private label credit card. ApplePay, Google Pay,[17] SamsungPay, and PayPal all offer general purpose wallets. Retailers like Starbucks (which offers the most widely used mobile wallet by far[18]), Walmart, and Amazon.com offer single-business wallets, as do online retailers that store consumers' payment information.

Second, how the wallet is funded varies. Some digital wallets are "open wallets" that can be linked to any payment source (credit, debit, or ACH with any payment network brand or bank). Others are "limited-open wallets" that can be linked to a limited number of payment sources. Still other digital wallets are "bank-open wallets" that can be linked to payment source offered by a specific bank, or "brand-open wallets" that can be linked to any payment source offered by a particular payment network. (In some cases, the wallet is both bank- and brand-specific.) And, finally, wallets can be "closed wallets" linked only to a single payment source from a single bank or brand. Thus far, all major single business and multi-business wallets have been open wallets or limited open wallets. Table 1 summarizes the spending and funding possibilities for digital wallets.

16 Digital wallets may differ in an additional dimension—the unit of account they use for transactions. This study does not address digital wallets that utilize so-called "cryptocurrencies": private, digital currencies, such as Bitcoin, that are usually based on blockchain technology.

17 Prior to 2018, Google Pay was two separate products: Android Pay (a pass-through wallet) and Google Wallet (a staged wallet). *See* Pali Bhat, *Bringing It All Together with Google Pay*, GOOGLE (Jan. 8, 2018), https://www.blog.google/topics/shopping-payments/announcing-google-pay/.

18 *See* Marcus Wohlson, *Forget Apple Pay. The Master of Mobile Payments is Starbucks*, WIRED (Nov. 3, 2014, 6:30 AM), https://www.wired.com/2014/11/forget-apple-pay-master-mobile-payments-starbucks/ [https://perma.cc/7SGY-R6QG].

Table 1: Digital Wallet Funding and Spending Possibilities

	Open Wallet	Limited-Open Wallet	Bank Wallet	Closed Wallet
General Purpose	ApplePay Google Pay Coin Masterpass PayPal SamsungPay Square Cash Venmo Zelle		Chase Pay Capital One Pay Citi Wallet (MC Only)	PAYTOO Wallet
Single-Business Wallet	Starbucks App Walmart Pay	Various Online Retail Wallets		
Multibusiness Wallet	Amazon.com Levelup Square Wallet (Defunct)	Currentc (Defunct)		

Third, digital wallets are either "pass-through" wallets or "staged" wallets. In a pass-through wallet, the digital device merely substitutes for a plastic card: instead of the payment authorization being stored on a card, it is stored on a phone or some other device. ApplePay and SamsungPay are pass-through wallets, and Google Pay offers a pass-through option.

Other wallets, however, such as PayPal, Square Cash, and Venmo, are staged wallets, and Google Pay can be a staged wallet, depending on the funding source used. A payment from a consumer to a merchant with a staged wallet is divided into two distinct legs. First, there is a funding leg, in which the consumer makes funds available to the digital wallet. The funding comes from whatever source the consumer selects—a bank account, a credit card, a line of credit from the staged wallet provider, or a payment balance on the staged wallet. The second leg moves the funds from the staged wallet to the merchant. This second leg may involve a different payment method than the first leg: the staged wallet might be funded through a credit card, but the payment to the merchant might be through ACH, thereby enabling the staged wallet provider to arbitrage the difference between its funding and its payment costs.

The staged wallet provider serves as an intermediary between the consumer and the merchant, accepting payment from the consumer and then relaying

payment to the merchant through a method of its own choosing.[19] Because the staged wallet provider stands between the consumer and the merchant, the merchant may receive different transaction information than if it transacted directly with the consumer. Similarly, the financial institutions involved in the funding leg see only the transfer to the staged wallet; they have no visibility into the identity of the ultimate merchant recipient.[20] Because of the two transactional legs in a staged wallet transaction, there is also the possibility of the consumer having a payment balance on the wallet—funds held by the wallet provider for the consumer, much like a bank deposit. Such payment balances are not possible on pass-through wallets.

Fourth, digital wallets vary by form factor. Form factor variation is a major functional distinction between traditional plastic cards and digital wallets. While all digital wallets are software based, some are accessed through web browsers, others through mobile device apps, and some through both. Web-based wallets store the consumer's payment data in the cloud and can be accessed by any device with a web browser, whether a desktop or a mobile device. Some web-based digital wallets, such as PayPal and Google Pay, are general-purpose wallets, which are not specific to any particular merchant. Most web-based digital wallets, however, are single-business wallets. And any merchant that stores consumer payment information in a way that it can be used for future transactions is offering a type of digital wallet. Thus many airlines, rental car companies, and Internet retailers offer digital wallets. Likewise, Amazon.com offers a multi-business wallet that can be used for payments to all Amazon.com sellers.

2. Mobile Wallets

Other digital wallets are "mobile wallets" that run on mobile devices, including smartphones, tablets, wearables, key fobs, and dongles. Some, such as Google Pay, ApplePay, and SamsungPay, are specific to the particular combination of software and hardware on certain devices. Others, such as the Starbucks app or PayPal, are apps that can run on multiple operating systems. Web-based wallets can of course be accessed from mobile devices, even if they

19 A similar intermediation role is played on the merchant side by merchant aggregators such as Square, Etsy, iZettle, WyzAnt, and Stripe. Some digital wallet providers, such as PayPal and Amazon, are also merchant aggregators. The consumer essentially makes the payment to the merchant aggregator, which then relays the payment to the merchant. The merchant aggregator business model is based on the merchant aggregator having a lower cost of receiving payments than the merchants themselves and arbitraging that cost spread. *Cf.* Alice Chen, *Merchant Account vs Processing Aggregators*, PAYFIRMA (Aug. 26, 2016), https://www.payfirma.com/grow-your-business/merchant-account-vs-aggregator/ [https://perma.cc/AHJ8-ZBPV]. *See generally* LERNER, *supra* note 2.

20 MasterCard and Visa have seen staged wallets as competitive threats. *See MasterCard's Wallet Fee: A Tool of Oppression, or One to Level the Acquiring Playing Field?*, DIGITAL TRANSACTIONS (Mar. 22, 2013), http://www.digitaltransactions.net/news/story/3928 [https://perma.cc/CEJ6-REQF]. In 2013, for instance, MasterCard imposed a fee on staged wallet transactions. *Id*.

do not have a specific mobile app (although some, like PayPal, do). Mobile wallets utilize a range of communications technologies for transmitting payment data from the device to merchants, including magnetic stripe emulation, NFC, Quick Recognition (QR) Code, Bluetooth, Bluetooth Low Energy, instant messaging, and the Internet.

Confusingly, some digital wallets have both web-based and app-based versions. Likewise, the same device, such as a smartphone, can host multiple digital wallets, which may utilize different communications technologies. For example, an iPhone user could use both ApplePay and a free-standing digital wallet application that would make payments over the Internet. Even more confusingly, some digital wallets are able to be included in other digital wallets. Thus, Capital One Pay can be used as a free-standing digital wallet or included inside an ApplePay wallet. At the same time, however, Apple does not make the NFC chip in iPhones available to third-party apps.[21] Thus, the only NFC-based digital wallet that can run on an iPhone is ApplePay, even though other digital wallets that do not use NFC can be used on an iPhone. In contrast, the NFC chip on Android devices is available to third-party developers.

C. *What Digital Wallets Change*

For payments processed through credit and debit card networks, digital wallets do not change the fundamental design of the five-party payment card system set up. Nor do they necessarily change the basic fee structure in the credit or debit card system, although they may reallocate some of the value in the system and possibly increase costs. To the extent that digital wallets provide the possibility of ACH payments, however, the fee structure is altered because in an ACH transition there are no interbank fees, only a small per transaction fee paid to the ACH operator.[22]

What digital wallets do change, irrespective of how the payments are processed, is the possible range of communication technologies for transmitting payment authorization from consumers to merchants and, more importantly, the format of the payment authorization data. These changes are significant because they may affect the flow and control of consumer data. Finally, digital wallets

---

21 *See* Rod Chester, *Big Banks Drop all Complaints but One in Last-Ditch Fight Against ApplePay in ACCC Inquiry*, NEWS CORP AUSTL. NETWORK (Feb. 13, 2017, 4:36 PM), http://www.news.com.au/technology/gadgets/mobile-phones/big-banks-drop-all-complaints-but-one-in-lastditch-fight-against-apple-pay-in-accc-inquiry/news-story/86437315691f6d8e5708d9793446f3e6 [https://perma.cc/WRY3-7NYV] (explaining how Australian banks fought Apple for NFC access). Apple appears to be moving to allow third-party NFC access. *See* Ben Lovejoy, *Apple Opening Up (Some) Access to the iPhone's NFC Chip in iOS 11*, 9TO5MAC (June 7, 2017, 4:00 AM), https://9to5mac.com/2017/06/07/apple-opening-up-some-access-to-the-iphones-nfc-chip-in-ios-11/ [https://perma.cc/W7F6-EEBU].

22 In an ACH transaction, the merchant's and consumer's banks may charge additional fees to the merchant and consumer, respectively.

potentially change payments from an isolated one-way data flow to a richer, two-way communications environment that encompasses the entire retail experience from advertising and search to purchase, shipping, returns, and customer loyalty.

1. The Method of Transmission of Payment Authorization Data from Consumers to Merchants

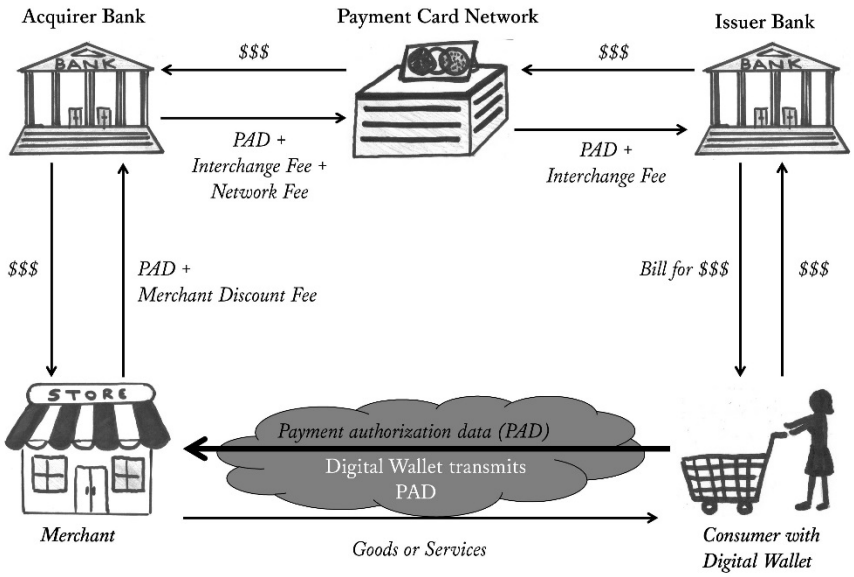
Digital wallets enable payments to be made from credit and demand deposit accounts using devices other than plastic credit and debit cards. In so doing, they expand the possible range of technologies used to transmit payment authorization from consumers to merchants. Transmission of the payment data in the rest of the payment network system (credit, debit, or ACH) remains unaffected by this change; ultimately, the consumer's bank will only authorize the transaction if the authorization data comes to it through a payment network in which it participates.

The traditional plastic payment card is merely an access device for an account, be it a demand deposit account or a line of credit. Accessing such an account requires transmission of proper authorization information to the bank that holds the account—the issuer. Access does not require a plastic card. Demand deposit accounts, for instance, do not require a plastic card for access; they may also be accessed by checks or by the account and routing number for ACH transactions. Likewise, even with a credit card account, authorization information can be transmitted in numerous forms by the consumer to the merchant, who then relays it to the issuer through a payment card network. For example, with a traditional card, the authorization data—the information on the front (and possibly the back) of the card—can be transmitted by swiping the card's magnetic stripe through a magnetic stripe reader, by oral transmission to the merchant (such as in telephonic transactions), by manual input (such as with entry of the card information in a website), or, in recent years, by "contactless" transactions using NFC.

Digital wallets potentially increase the possible methods for transmitting payment authorization data from a consumer to a merchant. Thus a digital wallet might use NFC technology, the Internet, text messaging, or magnetic stripe emulation for transmission of payment data.[23] The use of different data transmission technologies can potentially increase the risks faced by a merchant when accepting payments, as discussed later in subsection II.B.2.

23 The additional forms of data transmission are only feasible, of course, if a merchant is equipped to accept payments using such a technology.

Figure 2: Payment Card Transaction with Digital Wallet



2. The Nature of Payment Authorization Data

Digital wallets may also affect the format and nature of the information being transmitted from the consumer to the merchant, as well as from the merchant to the payment network. By altering the format and nature of the information transmitted, digital wallets may mask a cardholder's PAN and thereby deprive the merchant of the informational value of the transaction.

In a traditional credit or debit card transaction, the consumer transmits his unencrypted PAN as well as a static card verification value (either the CVV1 that is encoded on a magnetic stripe or the CVV2 digits written on the back of the card) to the merchant.[24] The merchant then relays the PAN and verification code information to its acquirer and thence to the network and, ultimately, the issuer for authorization. If a fraudster were to intercept or steal unencrypted payment authorization data either from the consumer or from any of the parties in the transmission chain, the fraudster could use it to create counterfeit physical cards or in fraudulent card-not-present transactions.

24 The precise terminology for the card verification value or card verification code varies by card network. For consistency, in this Article I refer to "CVV1" (static, magnetic stripe data), "CVV2" (static, back of card), and "CVV3" (dynamic, EMV-chip generated).

The Card Networks have encouraged adoption of security measures to address this fraud risk, although the particular measures encouraged have been questioned in terms of their effectiveness and distributional implications for participants in the payment systems. The two primary security responses to the risk of theft of payment data are (a) to reduce data retention by merchants and acquirers; and (b) to render payment data harder for thieves to use. Reducing data retention means that there is simply less payment authorization data sitting around for thieves to steal. Rendering data harder to use makes it less valuable and therefore less tempting to would-be thieves.

a. *PCI-DSS Mandated Encryption*

The mechanism for enforcing these security measures is the mandate of compliance with the Payment Card Industry Data Security Standard (PCI-DSS). PCI-DSS is promulgated by the Payment Card Industry Security Standards Council, an entity created and controlled by American Express, Discover, JCB International, MasterCard, and Visa.[25] The Card Networks require acquirer banks to ensure that merchants comply with PCI-DSS (and hold the acquirers liable for assessments upon noncompliance), so acquirers require merchants to attest compliance with PCI-DSS.[26]

A recent update to the PCI-DSS restricts data retention, providing that "[t]he only cardholder data that may be stored after authorization is the primary account number or PAN (rendered unreadable), expiration date, cardholder name, and service code."[27] Under PCI-DSS, "sensitive authentication data," such as card verification codes (the unembossed numbers on the back of cards), PIN numbers, and Full Track data (which contains all of the preceding data fields) may not be stored after authorization, even if encrypted.[28]

PCI-DSS also requires that any data that is retained be rendered less valuable for thieves through various methods of obfuscating data. In particular, PCI-DSS requires that the PAN (but not the cardholder's name, expiration date, or service

25 For more on the PCI-DSS standard, see Adam J. Levitin, *Private Disordering? Payment Card Fraud Liability Rules*, 5 BROOK. J. CORP. FIN. & COM. L. 1, 33-36 (2010).

26 *See, e.g.*, VISA CORE RULES AND VISA PRODUCT AND SERVICE RULES § 1.10.4.1 (2015) [hereinafter VISA CORE RULES], https://fronstream.zendesk.com/Inc/en-us/article_attachments/204224066/Visa_Core_Rules_And_Visa_Product_and_Service_Rules.pdf [https://perma.cc/45P9-ZGFG]. Historically the Card Networks have not required PCI-DSS compliance for smaller merchants. Since early 2017, however, PCI-DSS applies to small merchants as well. *See Small Merchant Security Program Requirements—UPDATE*, VISA, https://usa.visa.com/dam/VCOM/download/merchants/bulletin-small-merchant-security-faq.pdf [https://perma.cc/R9XJ-KDBU] (citing small merchant breaches by hackers as justification for applying PCI-DSS compliance protocols to smaller merchants).

27 PCI Security Standards Council, PCI-DSS 36 (Version 3.1 2015), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf?agreement=true&time=1506890639322 [https://perma.cc/WHM9-4MXE].

28 *Id.* at 37.

code) be rendered unreadable anywhere it is stored by encryption, hashing, or truncation methods.[29] PCI-DSS also requires that sensitive information be encrypted for transmission over open, public networks, like the Internet.[30] Therefore, once a merchant receives cardholder data, the portion of that data that is deemed "sensitive authentication data" should never be stored post-authorization, PANs should always be stored in encrypted form, and all sensitive data should only be transmitted in encrypted form. While this is not quite the same as mandating end-to-end encryption of all data, it achieves something similar.

PCI-DSS compliance is supposed to address the security vulnerability of cardholder data that a merchant has captured and retained, as well as the security vulnerabilities of transmission through open networks of cardholder data. Notably, however, PCI-DSS does not require that payment data be transmitted to the merchant in an encrypted form, unless it is transmitted over an open, public network like the Internet.[31] Transmission over in-house, private networks may still be done "in the clear" (i.e., unencrypted).[32]

b. *EMV Chip Cards*

PCI-DSS relies on encryption as its primary security method. Encryption involves using a mathematical algorithm to scramble data in such a way that only someone who has the decoding key can read the data. Another distinct security technology is the integrated circuit cards, also known as Chip or EMV cards. Chip cards contain a microchip that is used with a special card reader to verify that the card is genuine.[33] The communications channel in a chip card payment flows through the contact between the reader and the chip on the card. Chip cards, however, can also be "hybrid" cards capable of transmitting data via traditional magnetic stripe or NFC contactless technology, as well as through the chip.

---

29 *Id.* at 40.

30 *Id.* at 46-47. In addition to the Internet, PCI-DSS lists wireless technologies, cellular technologies, General Packet Radio Service, and satellite communications as a nonexhaustive list of open, public networks subject to encryption requirements. *Id.*

31 The lack of initial encryption for magnetic stripe transactions has the effect of putting the cost of encryption on the merchant, rather than on the card issuer, but allows the merchant to continue to have access to the PAN, and thereby retain the PAN's informational value for antifraud, advertising, loyalty, and customer service purposes.

32 Notably, although PCI-DSS does not require encryption for transmission on internal networks, it does not define what would constitute such a network. Data transmitted internally would necessarily be stored, however, so there should be some level of encryption or truncation of the data under PCI-DSS Requirement 3.4.

33 There is also an EMV contactless specification. *See generally* LERNER, *supra* note 2. It does not appear that any merchants in the United States currently accept EMV contactless transactions, meaning that all unauthorized transaction liability for transactions made using EMV contactless devices, such as ApplePay, is shifted to merchants. The lack of EMV contactless adoption appears to relate to the generally low rate of contactless acceptance in the United States and the certification costs of making contactless readers both EMV and PCI-DSS compliant.

When a Chip card is inserted in a Chip card reader, the microchip on the card generates a unique card verification code (CVV3) for each transaction based on a challenge-and-response interaction with the Chip card reader.[34] The transaction-specific CVV3 and the PAN are transmitted to the merchant in the transaction and sent ultimately to the issuing bank, which then uses them to authorize (or decline) the transaction.[35] The PAN and transaction-specific CVV3 are still transmitted in the clear from the Chip card to the merchant's terminal. Because Chip cards transmit unencrypted payment data to the merchant, PCI-DSS–mandated encryption is the main bulwark of defense against theft of payment authorization data from merchants.

It is often wrongly assumed that Chip technology prevents the creation of counterfeit cards. Although Chip technology makes it more difficult to counterfeit cards because the dynamic CVV3 on a Chip card can be used for only a single transaction, it does not prevent all counterfeit fraud.[36] Creating a fully functional counterfeit Chip card for an account would not be cost-effective: the cost of cracking the security would exceed the credit limit on almost any account. But the effectiveness of Chip technology as a security measure is reduced by the lack of a universal adoption mandate, the coexistence of the magnetic stripe authorization channel, the lack of domain specificity for PAN data, and the varying levels of card data verification used by issuers. The existence of multiple authorization channels that use data that is largely non-specific to any particular channel enables fraudsters to arbitrage the differences in security measures for each channel.

---

34 A hybrid card will still have a CVV1 encoded on the magnetic stripe and a CVV2 on the back of the card, but neither will be encoded on the chip or transmitted to the merchant in a Chip transaction.

35 Alternatively, the transaction can be authorized in an offline transaction by the merchant's EMV terminal, which matches a public encryption key against the private encryption key on the card.

36 Of course, several other types of fraud remain possible with EMV. *E.g.*, Ben Adida et al., Phish and Chips (Traditional and New Recipes for Attacking EMV), http://www.cl.cam.ac.uk/~rja14/Papers/Phish-and-Chips.pdf [https://perma.cc/WF67-JWQW] (explaining that data can be eavesdropped on from an EMV transaction, which can then be used to create a magnetic strip for fraudulent use in a foreign jurisdiction that does not support EMV); Ross Anderson & Mike Bond, The Man-in-the-Middle Defence, http://www.cl.cam.ac.uk/~rja14/Papers/Man-in-the-Middle-Defence.pdf [https://perma.cc/XS67-8VGZ] (describing how a middleman attack, whereby one merchant employs a relay device to monitor and forward chip and PIN information to an accomplice who is making another transaction, is not prevented by EMV technology); Black Hat, Crash and Pay: Owning and Cloning Payment Devices (2015), https://www.blackhat.com/docs/us-15/materials/us-15-Fillmore-Crash-Pay-How-To-Own-And-Clone-Contactless-Payment-Devices.pdf [https://perma.cc/UJ89-KPEG] (explaining the process of cloning EMV *transactions* in lieu of EMV *cards*); Mike Bond et al., Chip and Skim: Cloning EMV Cards with the Pre-Play Attack (Sept. 10, 2012), http://www.cl.cam.ac.uk/~rja14/Papers/unattack.pdf [https://perma.cc/LH7X-45BU] (noting that criminals have adapted to EMV technology in two ways: first by shifting to card-not-present transactions, and second, by cloning the magnetic strip of EMV cards); *see also* Thomas Fox-Brewster, *See How This Android App Clones Contactless Credit Cards in Seconds*, FORBES (Feb. 18, 2015, 12:05 PM), https://www.forbes.com/sites/thomasbrewster/2015/02/18/android-app-clones-cards/6433ff82db39 [https://perma.cc/VX8E-TT5E]; Peter Fillmore, Overview of Contactless Payment Cards (July 20, 2015), https://www.blackhat.com/docs/us-15/materials/us-15-Fillmore-Crash-Pay-How-To-Own-And-Clone-Contactless-Payment-Devices-wp.pdf [https://perma.cc/ED6K-SWUF].

For example, in a "milking" attack, a CVV3 and other authorization data could be lifted from a Chip card without a transaction being performed through a fake or altered terminal or RFID reader. That data could then be encoded on a magnetic stripe card and used at a non-Chip terminal or at a Chip terminal that reverts to a magnetic strip transaction when presented with a non-functional Chip card (a feature known as the "fallback function").[37] Indeed, it is even possible to encode the magnetic stripe such that the card appears to the reader to be "Chip-less," and thus the reader will not instruct the consumer to insert the card into the Chip reader slot.[38] While a diligent issuer should still catch such arbitrages based on differences in the service code for Chip and magnetic stripe transactions, issuers' verification procedures are not standardized.[39]

Moreover, even if a valid CVV3 cannot be captured, the PAN skimmed from a Chip card can be used in those card-not-present transactions that do not require a CVV2 because there is no domain specificity for PAN.[40] Thus one likely effect of the adoption of Chip technology will be the migration of fraud (or at least fraud attempts) from card-present transactions to card-not-present transactions, as well as to card-present merchants that do not accept Chip transactions.[41] So a more accurate statement of Chip technology's effect is that while it makes it not cost-effective to counterfeit a fully functional Chip card, it does not prevent all forms of counterfeiting because Chip card data can be used for magnetic stripe and card-not-present transactions.

All Chip cards and readers are made to conform to specifications from EMVCo, LLC. EMV is an acronym for the names of the venture's original partners: Europay International, MasterCard International, and Visa International. The current members of EMVCo are American Express,

37 *See* EMV Migration Forum, Understanding the 2015 U.S. Fraud Liability Shifts 2 (May 2015), https://signapay.com/images/resources/understanding_the_2015_us_liability_fraud_shifts.pdf [https://perma.cc/L2HS-978F]. For more on fallback functionality, see AMERICAN EXPRESS, IMPLEMENTING AMERICAN EXPRESS EMV™ ACCEPTANCE ON A TERMINAL § 4.1.1 (2007), https://www209.americanexpress.com/merchant/singlevoice/pdfs/chipnpin/EMV_Terminal%20Guide.pdf [https://perma.cc/WQW6-C7FH], and VISA, TRANSACTION ACCEPTANCE DEVICE GUIDE § 3.2.2 (2015) [hereinafter VISA TRANSACTION ACCEPTANCE DEVICE GUIDE], http://technologypartner.visa.com/download.aspx?id=32 [https://perma.cc/HJ8Q-FAZZ].

38 *See New Chip Card Security Flaw Found*, PYMNTS.COM (Aug. 4, 2016), https://www.pymnts.com/news/retail/2016/new-emv-security-flaw-found/ [https://perma.cc/T53Z-PD2A].

39 *Id*.

40 A notable exception is American Express, which does appear to have domain-specific tokenization. *See Frequently Asked Questions (FAQs): American Express Token Service*, AM. EXPRESS (Oct. 2014) [hereinafter *American Express Token Service*], https://network.americanexpress.com/globalnetwork/dam/jcr:480cdd06-048e-48a4-9b21-c65a18df2370/Token-Service-FAQs.pdf [https://perma.cc/F5FG-GT5F].

41 This was the experience with EMV adoption in the UK. *See* Bond et al., *supra* note 36, at 3.

JCB, Discover, MasterCard (which purchased Europay), UnionPay, and Visa—significantly, not the U.S. PIN-debit networks or ACH operators.[42]

The use of Chip cards and readers is not mandated in the United States, but it is encouraged by a change in the Card Networks' rules regarding liability for unauthorized transactions. In the United States, as of October 2015, American Express, Discover, MasterCard, and Visa (but not the PIN-debit networks, because they are not co-owners of EMVCo) instituted a change in their rules that allocate liability for unauthorized card-present transactions.

Historically, for card-present transactions (which include contactless transactions), the card issuer was liable for unauthorized transactions provided that the merchant followed the requisite security procedures.[43] Otherwise the acquirer would be liable for the unauthorized transaction, but would contractually transfer the liability to the merchant. In contrast, merchants have always been liable for all unauthorized transactions in card-not-present situations, although they can, by contract, shift the liability to other parties, such as the Card Networks, for card-not-present authentication services.

Under the revised rules, called the "EMV liability shift," if a consumer presents a Chip card in a card-present situation, liability for counterfeit card transactions shifts to the acquirer (and thence to the merchant) unless the merchant properly uses a Chip card reader, in which case the liability shifts back to the issuer.[44] The old rule that issuers are liable for counterfeit card-present transactions remains in place if the card presented is not a Chip card, as well as for unauthorized transactions not involving counterfeit cards.[45] By issuing EMV cards, issuers are thus able to shift the fraud risk for counterfeit cards to merchants. Although EMV cards cost more to issue than traditional magnetic stripe-only cards, most issuers appear to have determined that the savings from

42 *See Overview of EMVCo*, EMVCO, https://www.emvco.com/about/overview/ [https://perma.cc/MGBQ7-7359].

43 *See* Levitin, *supra* note 25, at 15.

44 *See* MASTERCARD, CHARGEBACK GUIDE § 3.5 (2014), https://www.mastercardadvisors.com/content/dam/advisors/en-us/documents/ChargebackGuide.pdf [https://perma.cc/XE4W-PXV3]; VISA CORE RULES, note 26, §§ 4.1.22.56, 5.9.2.5.

45 VISA CORE RULES, *supra* note 26, § 4.1.22.57. ATMs and automatic fuel dispensers are also not covered by the October 2015 liability shift. In order to avoid the liability shift, a merchant must properly use terminals that are certified as EMV-compliant. The EMV-certification process is by device type for each acquirer, and any kernel change in a device from a reprogramming, such as adding a new implementation allowing the terminal to accept PayPal, requires a new certification. The certification process has significant costs, and it is unclear how long an EMV certification remains valid absent a merchant's reprogramming of a device. Moreover, the initial transition to EMV has been slowed because the certification capacity is insufficient for the demand, resulting in a certification backlog. As a result, many merchants with EMV-capable terminals have not activated the EMV capability since it will not result in avoidance of the liability shift and will only result in slower transactions at point-of-sale.

the liability rule shift outweigh the issuance cost, especially when reissuance is done as part of the normal card replacement cycle.[46]

Despite the EMV liability shift, magnetic stripe technology is still widely used in the United States, even though it will presumably be phased out at some point in the future.[47] For the time being, however, the Chip and magnetic stripe technologies operate side-by-side. Many cardholders still have magnetic stripe–only cards. Issuers are replacing magnetic stripe–only cards with hybrid cards that can be used for both magnetic stripe and Chip transactions, but the replacement appears to be part of the normal card replacement cycle. Even with hybrid cards, however, many merchants have not installed or activated EMV card readers because of the high cost of the equipment and the subsequent PCI-DSS and EMV-compliance certifications, relative to the merchant's own antifraud benefits.[48]

Another reason for limited adoption of Chip acceptance is that part of the benefit from a merchant's use of Chip technology is the protection it provides to *other* merchants by reducing the likelihood that a data breach at the merchant will be used for fraud at those other merchants. In this regard, adoption of Chip technology is analogous to vaccination, in that it not only protects the vaccinated individual, but it creates positive externalities for other unvaccinated individuals in that the vaccinated individual cannot infect them. Merchants, however, are unlikely to account for this positive externality when making their decisions about accepting Chip transactions, and neither merchants nor issuers are mandated to use Chip technology. The lack of universal adoption combined with the continued use of magnetic stripe technology undercuts the potential effectiveness of Chip technology by creating opportunities to arbitrage security measures between authorization channels. Still, as Chip transactions become more common, fraudsters are likely to concentrate their attention on merchants

46 *Cf. How Much Will EMV Really Cost Issuers?*, PYMTS.COM (Sept. 3, 2014), https://www.pymnts.com/news/2014/how-much-will-emv-really-cost-issuers/ [https://perma.cc/PKW29ZAP].

47 *See* VISA TRANSACTION ACCEPTANCE DEVICE GUIDE, *supra* note 37 (noting that "Visa is currently evaluating time frames under which to establish a sunset date" for magnetic stripe technology); *EMV Contactless Acceptance Requirements*, VISA BUS. NEWS (Apr. 16, 2015), https://www.visa.com/chip/merchants/grow-your-business/payment-technologies/credit-card-chip/webinar/resources/webcast7/story_content/external-files/A104336.pdf [https://perma.cc/4E95-UEVE] (describing the industry shift towards chip technology and announcing future compliance deadlines). As merchants shift to EMV technology, though, it is not clear how the cause of fraud (including counterfeit, lost card, stolen card, fraudulent card application, and account takeover) will be determined. This raises the risk that merchants invest in the technology to become EMV compliant, but do not in fact avoid liability if the fraud is classified as due to something other than a counterfeit card.

48 *See* Ian Kar, *The Chip Card Transition in the U.S. has Been a Disaster*, QUARTZ (July 29, 2016), https://qz.com/717876/the-chip-card-transition-in-the-us-has-been-a-disaster/ [https://perma.cc/X9N7-952L].

that do not accept Chip transactions, thereby increasing the value to merchants of accepting Chip transactions.

The adoption of Chip technology does not affect merchants' ability to use PANs for antifraud, customer loyalty, advertising, and returns. Although the card verification code on a Chip transaction is dynamic, the cardholder's PAN is not, and is unencrypted when transmitted to the merchant.[49] This means that with Chip transactions, the merchant can correlate different transactions made with the same PAN, which facilitates antifraud, customer loyalty, and returns.

Digital wallets can, but need not perform Chip transactions. Some mobile wallets like ApplePay use a chip in the mobile device as the EMV chip for card present transactions, where the consumer is face-to-face with the merchants. The ability for a mobile wallet to do a Chip transaction, however, depends on the communications channel used by the wallet; web-based wallets, for example, cannot do Chip transactions.

c. *Tokenization*

Another security measure is "tokenization": the replacement of payment card data—the PAN and the card verification code—with randomly generated substitute data known as a "token." The token looks like a PAN and card verification code in that it contains the same number of digits, but it is in fact a random number that does not match any actual PAN, so it cannot itself be used for a subsequent transaction.

Unlike encryption, tokenization does not scramble data using algorithmic transformations. Instead, tokenization replaces the original data with randomly generated substitute data. The match between the random token value and the original data is recorded in a secure codebook (called a "vault") retained by the issuer. Tokenization, according to Visa's CEO, is "the single biggest change that's been made in the payment networks easily over the past 15 or 20 years and maybe longer."[50]

Tokenization is not a necessary feature of digital wallets, but it appears to be an increasingly standard security measure. By the same token, tokenization is not specific to digital wallets; it can be used by a merchant for any transaction as part of a layered security approach. For example, a merchant can transmit encrypted payment data to its acquirer. The acquirer will forward the encrypted PAN and card verification code to the Card Network and the issuer for authorization, but will itself (or through a vendor) tokenize the data and return only a token to the merchant. The merchant will retain

49 *See supra* Section I.A.

50 *VISA CEO Confirms Tokens as New Network Revenue Stream*, PYMNTS.COM (Nov. 13, 2014), https://www.pymnts.com/2014/visa-ceo-confirms-tokens-as-new-network-revenue-stream/ [https://perma.cc/NB2F-RRFW].

the tokenized data, rather than the original encrypted PAN and card verification code. This tokenized data is useless not only to the hackers, but also to the merchant.[51] Digital wallets potentially mask PANs by facilitating data "tokenization" before the data is even transmitted to the merchant.

It is possible, however, to use a "multipay" token that is unique to both a PAN and a merchant.[52] A multipay token is essentially a merchant-specific ersatz PAN. Such a multipay token can be used for subsequent transactions, including refunds and credits, but only at a single merchant. This is a solution that is often deployed by eCommerce merchants that store payment information in online digital wallets. After the initial transaction, the token will be linked with a description such as the card brand and the last four digits of a PAN. When the consumer selects the card with that particular description, the merchant will transmit the corresponding token to the acquirer, which will decode the token and transmit the original PAN and card verification code to the issuer for authorization. Digital wallets offered by eCommerce merchants thus frequently use multipay tokenization.[53] A multipay token also enables merchants to track a consumer's transactions for antifraud purposes, and—if the merchant can correlate customer address or other identification information with the token—advertising and loyalty program purposes.[54]

Tokenization is also used by offline digital wallets. The particular application of tokenization varies by digital wallet, but its use in the ApplePay digital wallet is instructive. When a consumer loads a card on the ApplePay digital wallet, the consumer first enters her card information in the ApplePay application on an iOS device. When the consumer does so, the iOS device communicates with Apple, indicating from which bank Apple should request a token and card verification code algorithm. In response to a request from Apple, the bank transmits the token and card verification code algorithm to Apple, which then re-transmits the token and card verification code algorithm to the iOS device. The token and card verification code algorithm are then stored by the iOS device on a special, dedicated microchip known as a "secure element" that cannot be accessed by iOS applications other than

51 This sort of acquirer tokenization does not eliminate data breach risk, but instead transfers it from the merchant to the acquirer, a sensible move only to the extent that acquirers maintain better security measures than merchants.

52 *See generally* FIRST DATA, HOW MULTIPAY TOKENS CAN REDUCE SECURITY RISKS AND THE PCI COMPLIANCE BURDEN FOR ECOMMERCE MERCHANTS (2012), https://www.firstdata.com/downloads/thought-leadership/MultipayTokensWP.pdf [https://perma.cc/N2JS-UDSF].

53 Multipay tokenization can even be done with a Chip card as long as the initial Chip card verification was done offline.

54 A multipay token does, however, create the risk of "on-us" fraud following a data breach using the multipay token at the merchant.

ApplePay. Only the token and the card verification code algorithm are stored on the iOS device; the cardholder's PAN is not stored on the iOS device.[55]

When a consumer authorizes a transaction—for example, through a fingerprint scan or entry of a PIN in ApplePay, the secure element is prompted to take the token and encrypt it using the card verification code algorithm. Although the token is itself static, the card verification code algorithm uses it to produce a unique cryptogram for every transaction, just as with a regular "Chip" card. ApplePay transmits the encrypted token to the merchant either through NFC or through a web browser.[56]

Tokenization plus encryption means that there are effectively two levels of data obfuscation between the cardholder's PAN and the cryptogram that is transmitted to the merchant. The cryptogram received by the merchant is an encrypted token, with an algorithmic relationship between the cryptogram and the unencrypted token, and a random relationship between the token and the PAN.

After ApplePay transmits the cryptogram to the merchant, the merchant (through its acquirer) retransmits it to the payment card network. The network will apply the card verification code algorithm to unencrypt the cryptogram, which, if the cryptogram is authentic, will produce the token. If the cryptogram is authentic, then the network will pass the unencrypted token along to the issuer, which will decode the token, producing the PAN of the cardholder attempting the transaction. Once the issuer determines that the token is authentic and that a transaction is authorized for the associated account, the issuer will authorize the transaction. All of this takes place in a matter of seconds.

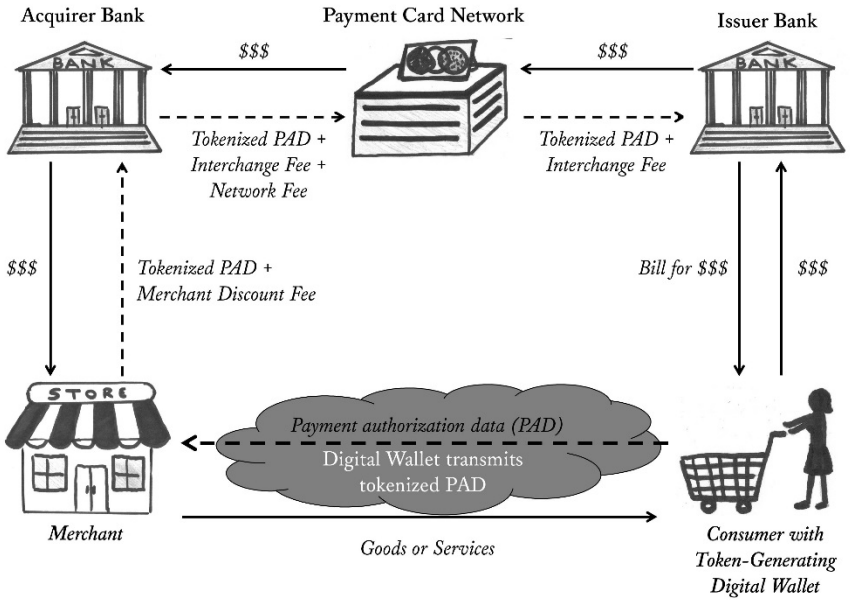
The basic mechanics of a tokenized transaction are similar to that of a regular magnetic stripe or Chip card transaction, but in a tokenized transaction, the merchant never sees the cardholder's PAN. Instead, the merchant has access to only a dynamically encrypted token. Thus, the merchant is not able to track transactions from the same consumer, frustrating antifraud measures, advertising and customer loyalty programs, and potentially even returns. Figure 3 shows how a token-generating digital wallet fits in a payment card network.

---

55 Access to the secure element is controlled by either the device manufacturer (Apple) or the mobile carrier (Android devices), which allows exclusion from the secure element of applications not approved by the device manufacturer or mobile carrier. On Android devices, however, a technology called Host Card Emulation enables use of a cloud-based secure element, thereby opening up the device to any application's use of a secure element. *See* E.J. House, *Tokenization a Critical Security Technology for Apple Pay and Other Mobile Payments*, 3 DELTA SYS. (Oct. 13, 2015), https://www.3dsi.com/blog/tokenization-a-critical-security-technology-for-apple-pay-and-other-mobile-payments/ [https://perma.cc/7SCS-M9BV].

56 *Id*.

Figure 3: Payment Card Transaction with Token-Generating Digital Wallet



3. The Economics of Payment Card Transactions

a. *Fees*

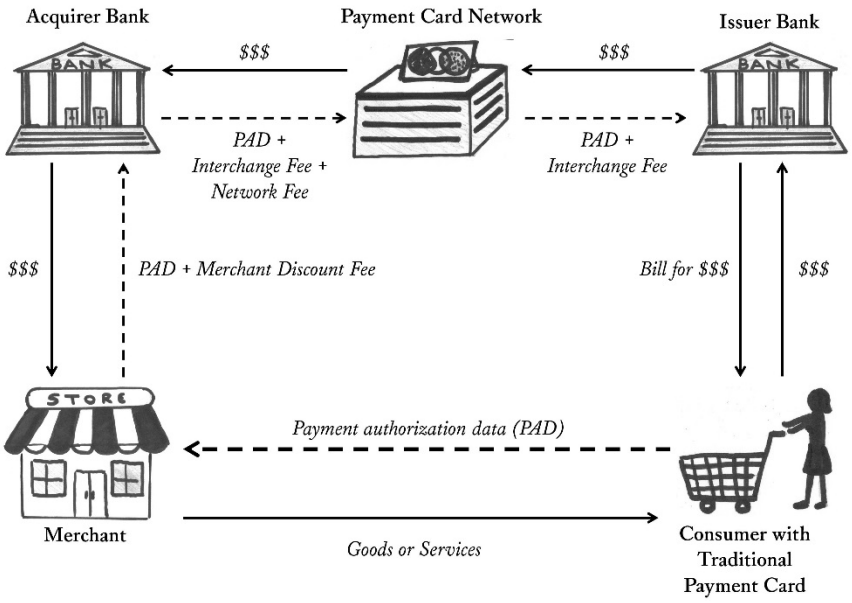
Digital wallets may also affect the economics of payment card transactions because they represent another mouth to feed in the transactional ecosystem. Services such as tokenization are not free. The parties that provide the digital wallet expect to be compensated, and their compensation will either come out of the pockets of acquirers, issuers, and the payment card networks, or will be passed on to merchants or to consumers. For example, on every ApplePay transaction, the card issuer reportedly pays Apple fifteen basis points (0.15%) on the transaction volume.[57] Those fifteen basis points eat into the issuer's bottom line. As the volume of ApplePay transactions increases, issuers will surely look to recoup those fifteen

57 *See* Jim Daly, *Apple Pay: No Charge for Merchants, But Transaction-Security Fees for Issuers*, DIGITAL TRANSACTIONS (Sept. 11, 2014), http://www.digitaltransactions.net/apple-pay-no-charge-for-merchants-but-transaction-security-fees-for-issuers [https://perma.cc/GN6V-LF2B] (noting Apple justifies the fee as a guarantee of the validity of the transaction).

basis points elsewhere. Similarly, the Card Networks themselves have indicated that they see digital wallets as a potential revenue source.[58]

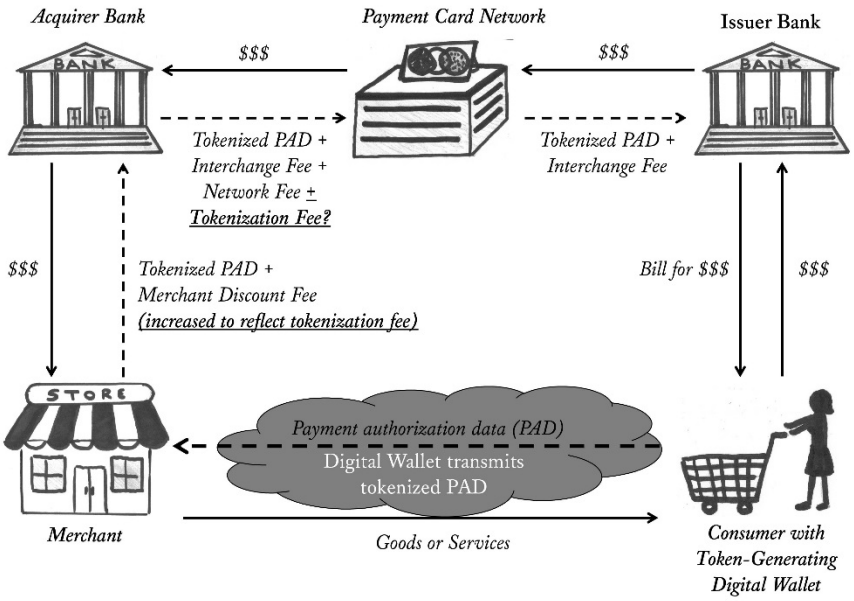
To the extent issuers or networks have increased expenses or seek to increase their own revenue, the result will likely be higher costs for acquirers. Demand for network services appears to be greater for acquirers (and thus merchants) than for issuers (and thus consumers) given that fees currently flow from acquirers to issuers in almost all payment card systems. Therefore, it seems likely that the costs of digital wallets will fall on acquirers in the first instance. To the extent that the costs of digital wallets fall on acquirers, the acquirers will, in turn, likely pass along the increased costs to merchants in the merchant discount fee, which is often structured as an express pass-through of the fees paid by the acquirer plus an additional mark-up percentage. Figures 4 and 5 show the fee structure for a traditional payment card transaction and for a digital wallet transaction.

Figure 4: Traditional Payment Card Transaction Economics



58 *See VISA CEO Confirms Tokens as New Network Revenue Stream*, *supra* note 50 (noting that although Visa waived tokenization fees for 2015, the company retained the ability to make "decisions on who you want to give access to, whether you want to charge for it and things like that").

Figure 5: Payment Card Transaction Economics with Digital Wallets



b. *Monetizable Data*

Digital wallets affect payment card economics in ways beyond fees. They also affect the flow of data in payment card transactions. Consumer data is a hugely valuable byproduct of payment transactions. It can be analyzed for marketing purposes, as payment data tells what a consumer has been interested in purchasing and what they are willing to pay for it. This data can be utilized by a wide range of merchants, including those that generate the data, their competitors, and even merchants in other sectors, including financial institutions. Yet if general consumer information is digital gold, payment information is digital platinum: it is information about how consumers actually spend, and past spending is often indicative of future spending. It is data already linked with monetization.

In a traditional plastic card transaction, most of the valuable consumer data—what particular items were purchased and at what price—is retained by the merchant and not shared with the Card Network or issuer bank. Instead, the financial institutions involved in the transaction see only an aggregate level of spending, the name of the merchant, and a general category label for the merchant. Absent a merchant's agreement, they cannot see item-level data

(also known as stock-keeping unit (SKU)–level data or Level 3 data).[59] Digital wallets can potentially reallocate that valuable data from the merchant to either the Card Network or the issuer. The ability of digital wallets to reallocate data is discussed in more detail in subsection II.B.2.a.

II. BENEFITS AND RISKS OF DIGITAL WALLETS

Digital wallets affect consumers and merchants quite differently. As we have seen, different digital wallets entail different form factors, technologies, and business models. Different digital wallets collect and transmit different data through different "pipelines." Accordingly, there are different risks involved with different digital wallets.

For consumers, different wallets present different profiles in terms of privacy and data security and—mirroring the credit/debit card distinction—different legal regimes for term disclosure, unauthorized transaction liability, and error resolution. For merchants, different wallets present different risks in terms of competitive impact and control over customer data, customer relationship management, control over tender choice and payment routing, fraud, data security, intellectual property liability, and cost.[60]

The differences matter to consumers, but not nearly as much as they do to merchants because of the differences in the underlying legal regimes. The consumer-to-merchant leg of the payment transaction is governed by a robust set of federal statutes and regulations. To the extent that existing public law for credit and debit card transactions carries over to digital wallets, as it presumably does and should, digital wallets have a more limited impact on consumers' legal rights.

In contrast, the merchant-to–payment system leg of the transaction is almost entirely governed through private ordering.[61] Merchants have only two protections against assumption of unwanted risks from digital wallets: they can simply refuse to accept digital wallets; or second, they can attempt to shift risks through contracts, whether through risk allocation with counterparties or

---

59 *See Visa's Next Big Business: Tokens and Data*, PYMNTS.COM (Sept. 25, 2014), https://www.pymnts.com/in-depth/2014/visas-next-big-business-tokens-and-data/ [https://perma.cc/3PNF-56KF] (explaining that although Visa's "network has the capability to capture SKU-level data and add that to the series of data and analytics services we can provide . . . . you would have to have an individual agreement with that merchant to capture that SKU-level data"); *see also Level 3 Processing*, BLUEPAY, https://www.bluepay.com/payment-processing/gateway/level-3/ [https://perma.cc/DD7J-E5UM] (contrasting the standard "level one" card data providing limited purchase data with "level three" data providing information akin to an "itemized invoice").

60 *See supra* note 1.

61 The sole exception is the Durbin Interchange Amendment, 15 U.S.C. § 16930-2 (2012), which places a cap on debit card swipe fees and requires multihoming for debit cards to encourage price competition for routing below the cap.

insurance. Neither of these protections is particularly effective, because, as subsection II.B.3 explains, the Card Networks' "Honor All Wallets" rules largely deprive merchants of their ability to refuse or condition acceptance of digital wallets.

A. *Consumer Benefits and Risks*

1. Consumer Benefits from Digital Wallets

Digital wallets hold out important benefits to consumers: faster and more convenient payments; improved recordkeeping; the integration of payments with loyalty and rewards programs; and helpful, targeted advertising and promotions.

Digital wallet payments can *potentially* be faster than traditional card payment. In particular, for EMV transactions, digital wallet payments made via NFC are faster than those made with a chip card using an EMV terminal.[62]

Digital wallets can also help consumers with their recordkeeping and accounting. By storing a record of consumer transactions, digital wallets can facilitate consumer returns, exchanges, and reimbursements, as well as assist with taxkeeping and personal financial planning. Paper receipts are bulky, require organization, and are easy to lose. A digital wallet can keep all of a consumer's receipts in one place, permit search and sorting, and takes up no additional space. Digital wallets can also provide data transfers to other software applications, such as personal finance applications like Quicken, that can be used for keeping track of a consumer's finances both generally and specifically for tax preparation.

Convenience (and coolness) is also a benefit for consumers. Rather than a bulky wallet full of store loyalty cards or a key chain covered with miniature reward program tags, a digital wallet can store information for multiple rewards and loyalty programs without taking up any more physical space. And although separate physical rewards and loyalty cards are easy to forget to use, a digital wallet can automatically apply rewards and loyalty programs with payment. Another convenience is that some digital wallet apps allow a customer to "order ahead" so that the order is ready when the customer arrives at the merchant's store.

Digital wallets also facilitate targeted promotions and advertising, which can benefit consumers. These promotions can be integrated with payments so that they are automatically applied when transacting, and targeted advertising can help consumers find products they might be interested in. Likewise, consumers can benefit from advertising and promotions because merchants are able to focus their promotions on the consumers most likely to use their products and to tailor their promotions toward those consumers' interests.

---

62 *See* Chen, *supra* note 19.

2. Consumer Risks from Digital Wallets

Digital wallets are not without risks for consumers. Though many of the risks apply generally to all payment systems, this subsection highlights additional risks specific to digital wallets.

a. *Varying Legal Regimes*

One of the risks related to digital wallets is the possibility of a shift in the governing legal regime. Different payment methods are subject to different legal regimes—the Truth in Lending Act (TILA) and Regulation Z thereunder govern credit cards,[63] the Electronic Fund Transfer Act (EFTA) and Regulation E thereunder govern debit cards,[64] and ACH transactions are governed by the private rules of the National Automated Clearinghouse Association (NACHA)[65] and potentially EFTA/Regulation E, depending on the particular transactional details.[66] These statutes and regulations provide a legal framework for disclosure requirements, liability for unauthorized transactions, and resolution of errors and system malfunctions. The TILA/Regulation Z rules for credit cards vary somewhat from the EFTA/Regulation E rules for debit cards and NACHA Rules. For example, consumers' unauthorized transaction liability for credit cards is capped at $50;[67] for debit cards it varies between $50, $500, and unlimited liability, depending on the consumer's negligence;[68] and under NACHA rules there is no consumer liability for unauthorized transactions.[69]

Presumably, the application of TILA/Regulation Z or EFTA/Regulation E does not change based on the form factor of the payment device used, at least for pass-through wallets like ApplePay, where the digital device merely substitutes

---

63 15 U.S.C. §§ 1601–1665 (2012); 12 C.F.R. § 1026 (2017). TILA/Regulation Z may well also apply to mobile carrier billing for third party charges, which operates much like a charge card account. *See generally* MARK E. BUDNITZ, THE LEGAL FRAMEWORK OF MOBILE PAYMENTS (2016), http://www.pewtrusts.org/~/media/assets/2016/02/legal_framework_of_mobile_payments_white_paper.pdf [https://perma.cc/8H2Y-VX5L].

64 15 U.S.C. §§ 1693–1693r (2012); 12 C.F.R. § 1005 (2017). General purpose, reloadable prepaid cards do not clearly fall within this legal regime, but are subject to a rulemaking by the Consumer Financial Protection Bureau that recently went into effect in October 2017. *See* Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z), 81 Fed. Reg. 83,934 (Nov. 22, 2016) (to be codified at 12 C.F.R. pts. 1005 and 1026).

65 *See Introduction* to NACHA, 2013 NACHA OPERATING RULES & GUIDELINES (2013). NACHA is a nonprofit association that serves as the ACH Network administrator. *See About NACHA—The Electronic Payments Association*, NACHA (2017), https://www.nacha.org/about [https://perma.cc/T9R7-YJWD].

66 *See, e.g.*, CFPB, SUPPLEMENT I TO 12 C.F.R. § 1005, at § 3(b)(1)(1)(i) (Nov. 14, 2016), https://www.consumerfinance.gov/eregulations/1005-Subpart-A-Interp/2016-24506#1005-3-b-1-Interp-1 [https://perma.cc/CDV6-49DA] (noting that ACH transfers by financial institutions to consumers are governed by Regulation E).

67 § 1643(a)(1)(B); 12 C.F.R. § 1026.12(b)(1)(ii) (2017).

68 § 1693g(a); 12 C.F.R. § 1005.6(b) (2017).

69 NACHA, *supra* note 65, § 3.11.

for the plastic card. TILA defines credit card as "any card, plate, coupon book or other credit device existing for the purpose of obtaining money, property, labor, or services on credit."[70] Thus, as the Fourth Circuit has observed, the "core element of a 'credit card' is the account number, not the piece of plastic."[71]

Similarly, while the application of EFTA is keyed to the use of an "accepted card or other means of access," and Regulation E is keyed to the use of an "access device,"[72] the two have identical definitions: "a card, code, or other means of access to a consumer's account."[73] The official CFPB interpretation of "access device" includes "debit cards, personal identification numbers (PINs), telephone transfer and telephone bill payment codes, and other means that may be used by a consumer to initiate an electronic fund transfer."[74]

While it would appear from these observations that TILA/Regulation Z and EFTA/Regulation E apply to digital wallets depending on the funding source of the payment, there is no case law yet on that point. Digital wallets do not affect the application of NACHA Rules because ACH is not a device-specific payment system.

And even if these legal rules do not change for pass-through wallets, they can still be a source of consumer confusion because a digital wallet might default a consumer's payment choice to a particular payment method, thereby selecting an applicable legal regime without the consumer realizing. For example, if a digital wallet contains both credit and debit cards, but the digital wallet defaults to the debit card, the consumer's liability for unauthorized transactions increases, even though the consumer may not have deliberately selected a debit card in the same way as when the consumer chooses which card to take out of a physical wallet. There is no possibility of default payment selection with physical wallets.

Staged wallets (such as PayPal) present an additional source of confusion in terms of the applicable legal regime. Recall that in a staged wallet there are two coupled transactions: a funding transaction and a payment transaction. The different stages of the transaction may well be subject to different legal regimes, something consumers are unlikely to know or understand. Suppose that the funding for a staged wallet transaction is from a debit card, while the payment transaction is through ACH. The funding transaction would be subject to EFTA/Regulation E. The payment transaction, however, would most likely to be subject to NACHA Rules.

The point here is that there may be some shift or confusion about which legal regime applies, and depending on the particular design of a digital wallet,

70 § 1602(k).

71 United States v. Bice-Bey, 701 F.2d 1086, 1092 (4th Cir. 1983) (finding that the use of a credit card account number over telephone qualifies as a "credit card" for TILA criminal fraud liability).

72 § 1005.6.

73 12 U.S.C. § 1693a(1) (2012); 12 C.F.R. § 1005.2(a)(1) (2017).

74 *See* CFPB, *supra* note 66, § 1005.2(a)(1).

there may also be a transformation in the applicable legal regime, which can impact consumers' rights in terms of disclosure requirements, unauthorized transaction liability, and error resolution. Consumers may well be unaware of these issues, and this bespeaks a need to consider greater uniformity in the regulation of different types of consumer payment systems, as well as a need to give consumers clear control over their default choice of payment source.

b. *Security Measures and Fraud Risk*

Digital wallets vary in terms of security measures: the consumer action needed to authorize the transaction, the sort of data stored, the sort of encryption or tokenization used, the applications that can access the consumer's data, and the ability to remotely disable or "wipe" the device with a "kill" switch. Moreover, some wallets are more easily hacked than others. As a result, there are different fraud risk profiles for different devices.

Consumers' direct pecuniary exposure to fraud risk is limited, however, for traditional plastic credit and debit cards, and as noted in the previous subsection, those same legal regimes would seemingly apply to credit and debit payments via digital wallet. There are, however, important indirect pecuniary and non-pecuniary costs for consumers when dealing with fraud, such as the hassle involved of notifying card issuers, getting cards reissued, and resetting automatic bill payments.[75] Thus there are still fraud risks to consumers from digital wallets. Indeed, to the extent that digital wallets store other consumer information, the impact of fraud can be greater—a fraudster might not only access the consumer's funds, but adding insult to injury, he might use the consumer's coupons, too.

Even within a particular digital wallet, there are security differences based on the type of payment made: for instance, a credit card or signature-debit card versus a PIN-debit card. Debit cards are legally required to "multihome," meaning being capable of processing transactions on more than one unaffiliated network.[76] Whether the consumer is defaulted by the Application Identifier (AID)—software on the merchant's point-of-sale terminal—to using a particular network (and thus a particular authorization technology), and whether the consumer understands the choice involved, both have implications for the fraud risk, because there is a much greater fraud risk for single-factor, authenticated signature-debit payments than for two-factor, authenticated PIN-debit payments. It is much easier for fraudsters to copy a card's magnetic strip than to copy a PIN and the one-time data from a chip, for example.

---

75 *See* Levitin, *supra* note 25, at 42.

76 *See* 15 U.S.C. § 16930-2(b)(1) (2012) (describing how a credit card issuer or card network cannot restrict the number of payment card networks on which electronic debit transactions may be processed).

The number of parties involved in digital wallet transactions might exacerbate fraud problems for consumers due to confusion about the proper party to contact when fraud is suspected. Consumers have little ability to sensibly evaluate the security measures on different devices so they cannot protect their interests with any type of security measure;[77] their main protection is the federal limits on direct pecuniary liability for unauthorized transactions.[78]

c. *Error Resolution*

An important part of the federal regulation of credit and debit cards are the regimes for addressing error resolution. Card issuers are obligated to investigate consumer claims of error in a timely fashion,[79] and consumers can withhold payment while such investigation is pending.[80]

With a traditional plastic card, it is very clear who the consumer should contact regarding an error. With a digital wallet, it is less clear. For example, would a consumer who had an error claim from a Chase Visa transaction using ApplePay know to contact Chase directly, rather than ApplePay or Visa? The problem is not the transformation of error resolution rights, but rather confusion in contacting the proper party. This confusion can result in delay (which changes legal liability regarding unauthorized debit card transactions[81]) or the consumer simply giving up, effectively depriving the consumer of her error resolution rights.

d. *Wallet Provider Insolvency*

Staged digital wallets such as PayPal, Venmo, and Google Pay allow consumers to maintain balances in their respective digital accounts. The funds in these accounts are not FDIC-insured; they are simply unsecured claims against the wallet-provider.[82] Thus in the event of PayPal, Venmo, or Google Pay's bankruptcy, there may be no recovery for consumers with account balances.

---

77 A recent enforcement action by the Consumer Financial Protection Bureau has underscored this and the need for digital wallet providers to be accurate in their claims about security. *See* Dwolla, Inc., CFPB No. 2016-CFPB-0007.

78 *See supra* text accompanying notes 67–69.

79 *See, e.g.*, 12 C.F.R. § 1005.11(b)–(c) (2017).

80 *See id.* at (c)(2) (listing the conditions for the provisional crediting of consumer's account for debit card transactions); 12 C.F.R. § 1026.13(d)(1) (2017) (listing the conditions when consumers can justifiably withhold payments for credit card transactions).

81 *See* 15 U.S.C. § 1693g(a)(2) (2012).

82 *See, e.g.*, GOOGLE PAYMENTS, TERMS OF SERVICE 13 (Aug. 31, 2017), https://payments.google.com/payments/apis-secure/get_legal_document?ldo=0&ldt=buyertos&ldr=US [https://perma.cc/95CZ-ADXJ] ("Funds held by GPC or its service providers (including any bank service providers) in connection with the processing of Payment Transactions are not deposit obligations of Buyer and are not insured for the benefit of Buyer by the Federal Deposit Insurance Corporation or any other governmental agency."); PAYPAL USER AGREEMENT 3 (July 27, 2017), https://www.paypalobjects.com/webstatic/ua/pdf/US/en_US/ua.pdf [https://perma.cc/

Wallet-provider insolvency presents a risk with pass-through wallets as well. Even if the wallet provider does not hold funds for the consumer, it still holds consumer data.[83] If a wallet provider were to become insolvent and cease operations, consumers would be cut off from any data stored in the cloud. This could include receipts for purchases and transaction histories, which would frustrate consumer attempts at product returns or accounting.

e. *Loss of Privacy*

Perhaps the most important difference in risks for consumers between traditional plastic cards and digital wallets is privacy. A consumer's spending habits are extremely revealing, conveying information about a consumer's interests and problems. As a saying often attributed to Martin Luther goes, "Show me where a man spends his time and money, and I'll show you his god."[84] Unsurprisingly, then, survey data indicates that privacy concerns are quite salient for consumers with mobile wallets.[85]

Traditional plastic cards do not offer the high level of anonymity of cash transactions. Nonetheless, they offer a reasonable degree of privacy insofar as they do not enable other parties to see the entire picture of a consumer's transacting behavior. A transaction with a traditional plastic card transmits only data about that particular transaction undertaken with that particular card. It does not transmit data about other transactions on that card or other cards, much less about the consumer's other behavior, such as the consumer's web browsing history.

A merchant to whom a traditional plastic card payment is made receives substantial information about that particular transaction. The merchant will know exactly what the consumer purchased (known as the "stock keeping unit" (SKU), or Level 3 data), for what price, and when.[86] But the merchant is limited in its ability to aggregate information from multiple transactions. At most, the merchant can aggregate other transactions the consumer has made using that particular card with that particular merchant. The merchant has no visibility into the consumer's other transactions at other merchants or using other payment

32CW-RUTK] ("Any PayPal balance you hold represents an unsecured claim against PayPal and is not insured by the Federal Deposit Insurance Corporation.").

83 *See, e.g.*, PAYPAL, PRIVACY POLICY FOR PAYPAL SERVICES (Mar. 29, 2017), https://www.paypal.com/us/webapps/mpp/ua/privacy-full [https://perma.cc/59H5-ERPZ] (noting how PayPal collects data from consumers through webpages they access, geolocation, and web cookies).

84 *E.g.*, *Martin Luther*, AZ QUOTES, http://www.azquotes.com/quote/798806 [https://perma.cc/DNU7-ZR99].

85 *See* CHRIS JAY HOOFNAGLE ET AL., MOBILE PAYMENTS (2012), https://www.ftc.gov/system/files/documents/public_comments/2013/12/00007-89102.pdf [https://perma.cc/BQ3H-SYCN] (describing how Americans overwhelmingly would reject any system that would track their purchases or share personal information with merchants).

86 *Id.* at 5-6 (noting how merchants receive significant data from card transactions but also that merchants cannot uniquely identify their customers).

cards, and the merchant will have no window into the consumer's payment history and account balances. And if the merchant is a brick-and-mortar retailer, it will also not have any visibility into consumers' web browsing and search history.

Conversely, with traditional plastic cards, financial institutions have much greater ability to aggregate information from transactions made at multiple merchants, even on multiple cards. But that information is still much more limited than what is available to merchants. With traditional plastic card transactions, neither the Card Network nor the consumer's bank ever sees the SKU data.[87] Instead, these institutions can identify the various merchants used by the consumer by whatever name the merchant uses; the merchant's industry by broad category (e.g., "Hardware Equipment and Supplies" or "Supermarkets");[88] and the manner in which the transaction was authorized (card-present or card-not-present), which provides some information about the consumer's past location.

To be sure, merchant category data can, in some cases, be quite revealing. Consider categories such as "Wig and Toupee Stores," "Massage Parlors," "Counseling Services—Debt, Marriage, Personal," or "Bail and Bond Payments."[89] One does not need to know the specific services purchased to get an impression of the consumer; some credit card issuers allegedly have used such information in their pricing algorithms.[90] But the level of consumer information revealed through merchant categories is also quite limited in many cases, such as with "Supermarkets" and "Book Stores." For example, a Card Network or card issuer would not be able to tell if a consumer's grocery store purchase was an ethnic food product (e.g., a Manischewitz or Goya brand product), if a consumer's pharmacy purchase was a contraceptive, or if a purchase from a "miscellaneous general merchandise" merchant was a sex toy. All that to say, with traditional plastic cards, specific consumption information remains obfuscated from the Card Networks and card issuers.

The result of this situation is that traditional plastic cards do not provide a comprehensive view of a consumer's purchasing habits. Instead, the consumer's transactional habits are divided into distinct silos. Although the consumer does

87 *Id.* at 6. Banks will offer merchants lower merchant fee rates in exchange for SKU-level data. *See, e.g.*, *Level 3 Processing*, *supra* note 59.

88 For a directory of classification codes used by Visa, see *Visa Merchant Category Classification (MCC) Codes Directory*, VISA [hereinafter *Visa MCC Directory*], https://www.dm.usda.gov/procurement/card/card_x/mcc.pdf [https://perma.cc/J43T-XUY8].

89 *See id.*

90 *See, e.g.*, Complaint at ¶ 75, FTC v. CompuCredit Corp., No. 1:08-cv-1976 (N.D. Ga. June 10, 2008). In that case, CompuCredit settled for an estimated $114 million in consumer restitution plus injunctive relief. Press Release, Fed. Trade Comm'n, Subprime Credit Card Marketer to Provide At Least $114 Million in Consumer Redress to Settle FTC Charges of Deceptive Conduct (Dec. 19, 2008), https://www.ftc.gov/news-events/press-releases/2008/12/subprime-credit-card-marketer-provide-least-114-million-consumer [https://perma.cc/C92M-CSUR].

not have privacy over particular transactions, she retains a certain level of privacy because no one has a detailed overview of her entire transactional life.

It is of course possible for data from individual transactions to be aggregated, but such aggregation is unlikely in the traditional plastic card context. Merchants are loathe to share their data with other merchants or financial institutions, and card issuers are loathe to share their cardholders' information with other issuers.

Digital wallets potentially change this privacy picture. A digital wallet can aggregate data on payments at multiple merchants using multiple payment accounts because all the data is stored in one place. It can also combine this data with data on the consumer's past web browsing and geolocation.[91] Digital wallets can even potentially add SKU-level data for transactions if the consumer uses a web- or app-based shopping cart, or if the merchant provides a digital receipt. Not all digital wallets collect or combine such information, but the possibility of such wide-reaching data collection substantially changes consumer privacy in commercial transactions. A much fuller picture of the consumer's search, location, and purchasing habits is potentially available through a digital wallet than through a traditional plastic card. The level of privacy that traditional plastic cards preserved through information siloing is thus readily lost with digital wallets.

Further, the integrated portrait of a consumer's transactional life is not the consumer's to control. It can be shared or sold with virtually any entity, and unlike merchants and card issuers, digital wallet providers can only readily monetize the data through sales to third parties.[92]

The data aggregation facilitated by digital wallets enables much more targeted advertising and rewards, which is a boon to some consumers. Not all consumers, however, want to part with their privacy or want targeted advertising and rewards, and the degree of control a consumer has over his or her privacy is likely to be limited and opaquely disclosed through general disclosures regarding the collection and sharing of data. Digital wallets thus pose a privacy risk to consumers. Consumers might be willing to part with some or all of their privacy, but by using a digital wallet, the consumer can easily lose control of her privacy to a degree that she may not anticipate or fully understand.

---

91 *Cf. Privacy*, GOOGLE, https://privacy.google.com/your-data.html [https://perma.cc/G5Q5-Z623] (describing how Google collects data from its users, including their websites browsed, locations visited, and videos watched).

92 *See* Brian Naylor, *Firms Are Buying, Sharing Your Online Info. What Can You Do About It?*, NPR: ALL TECH CONSIDERED (July 11, 2016, 4:51 PM), http://www.npr.org/sections/alltechconsidered/2016/07/11/485571291/firms-are-buying-sharing-your-online-info-what-can-you-do-about-it [https://perma.cc/5LHN-D8TX] ("There are some big companies out there that . . . know more about you than you can imagine . . . . There are few regulations governing these [data] brokers.").

3. The Need for a CFPB Digital Wallet Rulemaking

Consumers have limited ability to manage the risks posed by digital wallets and have no ability to bargain directly with wallet providers over terms and conditions. Instead, they can pick which digital wallet they prefer, or they can "just say no" and eschew the use of digital wallets altogether—at least for as long as they can continue to transact using traditional payment media.

The ability to pick among digital wallets generates some amount of competition, which can provide some protection for consumers by generating better terms. Some digital wallets are specific to a particular payment card or financial institution, and many are capable of piggybacking on accounts at a range of financial institutions and Card Networks.[93] Accordingly, consumers generally have extensive options when choosing among the various digital wallets in the market, and are not even bound to using only a single wallet. But competition is only likely to provide consumer protection when product terms are salient enough that consumers can in fact notice and use them to distinguish between different products. Consumer choice will not bring market pressure to bear on terms that are either non-salient or on which products cannot be differentiated.

And for security and privacy, unfortunately, there is little reason to think that market pressure is likely to be effective. Consumers have little ability to gauge the strength of different digital wallets' security features or to understand the privacy implications of different wallets given the broad data sharing language that is typically included in privacy disclosures. This suggests that there may be a role for regulatory intervention to mandate minimum security measures, deposit insurance coverage, and privacy standards for digital wallets.

The Consumer Financial Protection Bureau has both the jurisdiction and regulatory authority to codify the aforementioned suggestions regarding security measures, deposit insurance coverage, and privacy standards. It can use rulemaking to proscribe unfair, deceptive, and abusive acts and practices by "covered persons."[94] Covered persons are defined as persons who offer or provide consumer financial products or services,[95] including transmitting funds, providing stored-value payment instruments, and providing payments "by any technological means."[96] While there may be questions regarding the status of any particular

93 *See supra* Part I.

94 12 U.S.C. § 5531(b) (2012).

95 12 U.S.C. § 5481(6) (2012).

96 *Id.* at (15)(A) (defining "financial product or service" to include any payments or data processing by an technological means). There is a jurisdictional carveout for "electronic conduit services." *Id.* at (15)(C)(ii); *see also id.* at (11) (defining electronic conduit services as people other than the payor or payee in a transaction who electronically transfer consumer financial data but do not select or modify its content, or handle it differently from other types of data they transfer).

party involved in the provision of a digital wallet, it is impossible to provide a digital wallet without the involvement of one or more covered persons.[97]

The Bureau's authority over covered persons includes the authority to prohibit "abusive" acts or practices, such as those that take unreasonable advantage of (i) a lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service; (ii) the inability of the consumer to protect the interests of the consumer in selecting or using a consumer financial product or service; or (iii) the reasonable reliance by the consumer on a covered person to act in the interests of the consumer.[98]

Unclear legal regimes, security measures, deposit insurance, and privacy issues can all fit into these prongs. The governing legal regime is a material risk of a digital wallet. Consumers are unlikely to understand the particular details of the legal regimes governing different sorts of payments, and to the extent that a staged wallet results in a shift to a less favorable legal regime, it could be an abusive act or practice. The CFPB has already brought enforcement actions under the abusive power based on consumers' lack of understanding of the applicable legal regime for usurious loans and debt collection (including forum selection).[99] Based on these past enforcement actions, it is plausible to read the prohibition on "abusive acts or practices" to extend to digital wallets with unclear legal regimes, inadequate security measures, lack of deposit insurance, or overreaching data collection.

Security features are also a material risk of digital wallets. Consumers are unlikely to understand the particular security features on digital wallets.[100] Consumers are also unlikely to be able to distinguish between the strength of security features between digital wallets, which makes it impossible for them to protect their interests when deciding which digital wallet to use.[101] As a result, consumers might reasonably rely on digital wallet providers to act in their interests by using the best possible security measures.

Deposit insurance coverage is another material risk for some digital wallets. Consumers are able to maintain a balance on a staged wallet—funds

---

97 The CFPB also has authority over entities that provide services to covered persons, related parties of covered persons, and parties that provide substantial assistance to unfair, deceptive, and abusive acts and practices. *See* § 5531(a); *see also* § 5481(25)–(26).

98 § 5531(d)(2).

99 *See, e.g.*, First Amended Complaint at ¶¶ 69–71, CFPB v. CashCall, Inc., No. 1:13-cv-13167(GAO) (D. Mass. Mar. 21, 2014) (describing the defendants' actions that allegedly constituted abusive acts or practices under the CFPA, including attempting to take loan balances on loans rendered void by local usury and licensing laws); Complaint for Injunctive Relief at Damages at ¶¶ 74–78, 80–81, CFPB v. Freedom Stores, Inc., No. 2:14cv643ANA/TEM (E.D. Va. Dec. 18, 2014) (charging the practices that were allegedly abusive in violation of the CFPA, including filing debt-collection lawsuits in Virginia against consumers who did not understand or negotiate their contract's forum-selection clause).

100 *See Survey: Despite All the Digital Wallet Buzz, Few Consumers Understand or Use One*, DIGITAL TRANSACTIONS (Feb. 5, 2013), http://www.digitaltransactions.net/survey_-despite-all-the-digital-wallet-buzz-few-consumers-understand-or-use-one/ [https://perma.cc/A9RS-6P7F].

101 *Id.*

held for the consumer by the wallet provider. If the digital wallet provider were to fail, the consumer would be a general unsecured creditor of the wallet provider, with no guarantee of ever being able to access the funds, in contrast to an FDIC-insured deposit.

Consumers may be unaware that their balances on most staged wallets are not FDIC-insured because this fact is not prominently disclosed, in contrast to what is required for uninsured depository institutions.[102] Instead, the lack of federal deposit insurance for staged wallet balances is buried in the fine print of the user agreement, which few consumers are likely to view. The same transparency concern applies to all digital wallets in regard to ensuring the continued availability of consumer financial data in the event of insolvency, a risk against which consumers have no ability to protect.

Transactional privacy concerns also fit under alternative prongs of the "abusive" standard and present a material risk to digital wallet users. Consumers may well not understand the implications to their transactional privacy because of the unsiloing of data facilitated by digital wallets. Likewise, because of the vague and general enabling wording of privacy policies, consumers have little ability to differentiate between digital wallets in terms of actual practices, so they cannot protect their interests through consumption choices.[103]

All of this suggests that the CFPB, under its power to prohibit "abusive" acts and practices, can regulate digital wallets that do not meet minimum standards for clarity of legal regime, security features, deposit insurance coverage, and transactional privacy. What those minimum standards should be is beyond the scope of this Article, but such rules would likely facilitate, rather than constrain, the growth of the digital wallet market by giving consumers greater confidence in digital wallet products, just as limits on unauthorized transaction liability encourage consumer use of traditional credit and debit card products.

---

102 *Cf.* 12 U.S.C. § 1831t(b) (2012) (mandating depository institutions conspicuously and routinely disclose a lack of federal deposit insurance). Notably, the term "depository institution" reaches any entity the CFPB determines is in the business of receiving deposits or which could be reasonably mistaken for a depository institution by its customers. *Id.* at (e)(2)(B)(ii). This leaves open the possibility of the CFPB defining staged-wallet providers as depository institutions and thus requiring prominent disclosure of the lack of FDIC deposit insurance.

103 The CFPB also has rulemaking authority under the privacy provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6804 (2012), which "requires financial institutions to explain their information sharing practices to their consumers and to safeguard sensitive data." *Graham-Leach-Biley Act*, FTC, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/graham-leach-bliley-act [https://perma.cc/D4JT-3FZ8]; *see* 12 U.S.C. § 5481(12)(J) (2012) (noting that the Gramm-Leach-Bliley Act constitutes an applicable "enumerated consumer law"). Given the limited statutory scope of the Gramm-Leach-Bliley Act's privacy provisions, however, the CFPB would likely have to act under its UDAAP power. Chris Hoofnagle and others have proposed adopting a modified federal version of California's Song-Beverly Credit Card Act, which prohibits merchants engaging in mobile transactions from soliciting certain information from credit card–using consumers. *See* HOOFNAGLE ET AL., *supra* note 85, at 16-17.

B. *Merchant Benefits and Risks from Digital Wallets*

1. Merchant Benefits from Digital Wallets

For retailers, digital wallets offer some attractions as payment devices—in particular, potentially greater tender speed—but the real attraction of digital wallets goes beyond payments: digital wallets are the potential lynchpin for an integrated suite of retailing services covering the entire retail experience from advertising and consumer search functions to payment and shipping, returns, and loyalty programs.

In twentieth-century commerce, these various retailing services were splintered on multiple platforms. The consumer obtained information about products through a variety of channels, ranging from store windows to advertisements to Internet searches. The advertising and search functions were completely delinked from the payment process, and the payment process was not connected with tracking of shipping, returns, or customer loyalty programs. Thus in twentieth-century commerce, each retailing function was essentially siloed.

This siloing limited retailers' ability to exploit consumer data because no one in the purchasing chain had a complete informational picture. For example, a traditional brick-and-mortar retailer generally knows only about the sales it has made, not about consumers' unsuccessful searches. Moreover, even though that retailer is able to match the consumer's credit card purchases made using the same card by using the consumer's name and card number, the retailer is not able to match transactions made by the same consumer using different payment methods because consumer names are not unique. This is why some merchants use loyalty cards that provide a unique identifier for the consumer that can be used for all transactions, irrespective of payment method.[104]

Twenty-first century retailing involves the integration of these different functions into a single platform that provides search, payment, and relationship management functions. This integrated retail platform gives merchants greater ability to attract and retain customers. The integration of payments and communications can be very beneficial for both consumers and merchants, although it does raise important consumer privacy concerns.

Integrated retail platforms already exist for many eCommerce merchants. Amazon, for example, already provides a well-integrated platform for these services within its universe. Amazon provides advertising and a search function, it stores payment information in its own digital wallet, and it enables tracking of shipments and return processing on the same platform. In contrast, traditional retailers lack information about unsuccessful searches, repeat searches and purchases, items saved for later in digital shopping carts, and even how long consumers spend looking at particular products or placing their mouse on a particular product's

104 HOOFNAGLE ET AL., *supra* note 85, at 6.

portion of a display.[105] Twenty-first century commerce creates an incredible wealth of consumer information for merchants, and that information can be analyzed and monetized. Amazon has pursued this twenty-first century retailing model within a single firm that sells nearly everything.[106]

A successful integrated digital retail platform requires two-way communications. The consumer needs to be able to transmit a range of information to the merchant, and the merchant needs to be able to transmit a range of information to the consumer. This is not possible with a traditional "dumb" payment card. The traditional plastic card is a one-way communication device that transmits payment authorization data and nothing more. It is, by definition, not integrated into a larger retail platform. Putting such a card into a digital wallet, however, makes it possible to integrate payments into an all-encompassing retail services suite. Digital wallets promise to bring the online integrated retail experience into brick-and-mortar commerce through mobile devices.

While it is possible to offer many of the other services separately from payments, integrating payments into the retail suite makes the transaction more seamless for the consumer. This is important for retailers because the more seamless a transaction is, the less likely it is that the consumer will become distracted or have second thoughts and not go through with the purchase. For online retailers in particular, "abandoned carts" are a major problem—one index has found abandonment rates of 78%[107]—and most often at the payment stage.[108] One of the causes of abandonment is issues with payments—including excessive security checks and declines—that would not occur with a digital wallet.[109] Avoiding these issues by integrating payments into a retail platform should ultimately then result in more completed sales. Digital wallets thus affect not just payments but the very model of retailing.

---

105 *See* Lina M. Khan, Note, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 782 (2017) (noting that traditional stores cannot match the "scale and sophistication" of Amazon's information collection efforts).

106 Of course, there are other approaches too, including a platform that is not firm-specific, but instead covers almost everything by encompassing multiple firms through a single gateway. Amazon also presents this model with its third-party sellers, but the structure still allows Amazon to capture data on all sellers' sales.

107 *Listrak Shopping Cart Abandonment Index*, LISTRAK, https://www.listrak.com/digital-marketing_automation/multichannel-marketing-solutions/email-marketing/shopping-cart-abandonment-index.aspx [https://perma.cc/6Z3Q-VDTE].

108 Andrew Meola, *ECommerce Retailers Are Losing Their Customers Because of This One Critical Mistake*, BUS. INSIDER (Mar. 16, 2016, 2:48 PM), http://www.businessinsider.com/eCommerce-shoppers-abandon-carts-at-payment-stage-2016-3 [https://perma.cc/G9T9-CTD7] (noting that as many as 74% of online carts are abandoned at the payment stage, particularly because "consumers have little to no desire to manually enter all of their information").

109 *Why Online Retailers Are Losing 67.45% of Sales and What to Do About It*, SHOPIFY (Aug. 6, 2013), https://www.shopify.com/blog/8484093-why-online-retailers-are-losing-67-45-of-sales-and-what-to-do-about-it [https://perma.cc/V4ZU-QMSP] (noting eighteen percent of consumers abandon their shopping carts due to excessive payment security checks).

2. Merchant Risks from Digital Wallets

a. *Control Over Customer Data*

The single most important concern for merchants regarding digital wallets is the loss of control over customer data. Digital wallets are an informationally rich environment compared to traditional plastic cards. A digital wallet can potentially tie together information about a consumer's web searches, transactions (on multiple cards), physical locations (current and past), and contact information (such as email address and phone number). The collection of this linked information enables advanced consumer behavior analytics. It also creates a channel for realtime marketing communications. The consumer behavior data and communications channel can be combined, in turn, to produce very targeted advertising and offers for consumers.

The problem digital wallets present for merchants is that although merchants sow the seeds for the informational crop, they are not the ones who reap its harvest. The additional information about a consumer generated by a digital wallet is controlled neither by the merchant nor by the consumer. Instead, it is controlled by the digital wallet provider and/or the payment card network.[110] Indeed, because of tokenization, digital wallets can result in an informational diminution for merchants (as discussed in the following subsections). So despite the greater informational wealth created by digital wallets, merchants come out worse—not only does all of the additional value go to other parties, but digital wallet payments may produce less informational value for merchants than traditional card payments.

The problem merchants face, however, is not simply that other parties can harvest and harness the additional data generated by digital wallet transactions, but that nothing prevents digital wallet providers or the Card Networks from selling the data to third parties, including the merchant's competitors, who can then use it to poach the merchant's customer relationships. The merchants interviewed for this Article—all Fortune 500 firms—unanimously described this concern as among their most pressing.

For example, hypothetical fast food restaurant Tast-i-Fast could enter into a deal with a digital wallet provider under which Tast-i-Fast obtains information on all of

110 Aside from merchant issues, there is an additional level of competition between the Card Networks and independent digital wallet providers. The Card Networks have at times exercised their market power to ensure they are the entities that control the information generated by digital wallets. MasterCard imposed additional fees on "staged digital wallets," like those of Google Pay and PayPal, which do not pass along details of the transaction to MasterCard. These fees are meant to ensure that the data flows to MasterCard, so that it can construct a detailed profile of the cardholder's spending habits. *See* Sarah Clark, *MasterCard Fights Back Against New Payments Players with Increased Transaction Fees for Digital Wallets that Don't Share Data*, NFC WORLD (Mar. 20, 2013), https://www.nfcworld.com/2013/03/20/323195/mastercard-fights-back-against-new-payments-players-with-increased-transaction-fees-for-digital-wallets-that-dont-share-data/ [https://perma.cc/YH9N-JGNJ].

the digital wallet transactions at its competitor Quick-i-Serve. This is hardly what Quick-i-Serve wants—why should it be generating data for its competitor's benefit?

The possibility of the Card Networks selling data on a merchant's transactions to a competitor already exists with traditional plastic cards, though that information is of limited use. If Tast-i-Fast purchased traditional plastic card information from a network, it would generally not be able to link purchases made on different cards to the same consumer. Nor would it be able to link the information to either the consumer's web searches or physical location. These factors limit the analytical value of the information. Even if Tast-i-Fast could generate a compelling insight from its information to attract consumers away from Quick-i-Serve, it could not communicate that offer to the consumers in real time. At best, it could use targeted advertising and hope that the message would not decay between the time of receipt and the time of a purchase.

These limitations on linking and utilizing information disappear with a digital wallet. A digital wallet provider can sell a much richer selection of consumer data and realtime communication access to the consumer. Consider this scenario: Meg has used her smartphone-based digital wallet to purchase baby supplies and baby furniture. Meg now goes shopping at The Store, a large retailer. As soon as she enters The Store's parking lot, she receives this text message from her digital wallet provider: "Hi Meg! We see you're in The Store's parking lot. We wanted to let you know that TheWeb.com is offering diapers at ten percent less than The Store, and with free shipping, but only if you purchase in the next hour (through this link)." Not one to turn down a good deal, Meg selects the link, purchases the diapers online, and drives out of The Store's parking lot without even getting out of her car. The Store has lost her business to TheWeb.com.

How did this happen? Meg's digital wallet provider knows her general type of purchases, and is able to determine the stores she frequents, though perhaps not the exact items she purchases. It is also able to see her web searches, and because of a geolocation sensor in the smartphone, it can determine where Meg has gone and when. That allows the digital wallet provider to guess the types of items Meg might be interested in purchasing, and to identify when she is on the cusp of a potential purchase. That data can then be sold to a merchant, such as TheWeb.com, which can swoop in with a better offer for Meg (with access to Meg's device again provided by the digital wallet provider).

For Meg this might be a great deal: she has gotten cheaper diapers, and saved some time. But it is a bad deal for The Store, which loses a sale of diapers, any potential impulse buys Meg might make, and any revenue that would result if Meg would have paid for the purchase with The Store's private-label or co-branded payment card. The Store is getting scooped on these transactions because it has lost control over customer information because of the digital wallet.

Now consider the possibility that the digital wallet provider is itself a large online retailer. The scenario above would allow such a retailer to scoop business away from brick-and-mortar retailers. Brick-and-mortar retailers' fear over being scooped by online competitors is hardly a far-fetched scenario: Walmart is sufficiently concerned about Amazon obtaining data on its sales that it forbids its vendors from using Amazon cloud computing services.[111]

The Honor All Wallets rules, discussed later in subsection II.B.3, prevent the brick-and-mortar retailer from taking steps to protect its business from poaching via mobile devices. If the brick-and-mortar retailer accepts Visa payments through NFC, it must accept them from all Visa NFC devices, ranging from NFC-enabled plastic cards to NFC digital wallets, including digital wallets offered by its competitors. Thus if Amazon were to offer an NFC-based digital wallet (to which it could potentially migrate the 150 million or so payment accounts it already has in its web-based digital wallet), brick-and-mortar retailers that take NFC payments would have to accept it and give Amazon access to their customer information.

Payment companies that employ co-branded cards (e.g., a United Airlines Visa) already have insight into customer behavior, but a smartphone digital wallet is a realtime communications channel with geolocation, enabling timely and targeted offers, advertisements, and coupons in a way that a co-branded card does not. Moreover, with a co-branded card, the consumer must sign up (and qualify) for the card. Providing a digital wallet is much simpler; the consumer has already signed up and qualified for the card(s) and just has to put it in the wallet. Subsequently, the wallet provider or Card Network can gain a window into the transacting on all of the cards on the wallet.

Digital wallets thus present a material change in the terms under which a merchant transacts. When merchants transact with a digital wallet, they surrender data that might be used to poach their future sales. Every digital wallet transaction carries a set of competitive risks that traditional plastic cards do not. These risks are not necessarily identical for all digital wallets. Merchants, however, are forced to accept them all if they take any using a particular technology. Thus merchants receive materially less value with digital wallet transactions than with traditional plastic cards.

For some merchants, device-based digital wallets present an additional competitive threat. Some merchants already provide their own web-based digital wallets that store payment card authorization data. These merchants have made a major investment to get consumer data and now face disintermediation and loss

111 *See* Dennis Green, *IT'S WAR: Walmart Is Telling its Vendors to Stop Using Amazon's Cloud*, BUS. INSIDER (June 22, 2017, 12:02 PM), http://www.businessinsider.com/walmart-tells-its-tech-providers-to-stop-using-amazon-services-2017-6 [https://perma.cc/KCQ3-PMNP]; *see also* Khan, *supra* note 105, at 755 ("Amazon gleans information from . . . competitors as a service provider that it may use to gain a further advantage over them as rivals—enabling it to further entrench its dominant position.").

of control over the data. For instance, while airlines are primarily card-not-present merchants, they do some business in card-present settings at ticket counters and on planes. Many airlines offer their own web-based digital wallets. If customers use competing digital wallets for card-not-present ticket purchases from a specific airline, the informational value of the airline's digital wallet diminishes.

b. *Customer Relationship Management*

Digital wallets can also interfere with merchants' ability to manage customer relationships. If a consumer is having difficulty transacting with a digital wallet, a merchant's sales associate is unlikely to be able to assist, because the sales associate may not be familiar with that particular wallet. The customer, however, might still hold the merchant responsible for his or her inability to transact and be reluctant to patronize the merchant again.

When digital wallets tokenize payments, further customer relationship management issues may emerge. With a tokenized payment, the merchant sees only the token, not the PAN. Merchants use PANs for a variety of purposes including returns, chargebacks, product safety recalls, loyalty programs, fraud prevention, and anti–money laundering compliance. Tokenization interferes with these applications of the PAN. For example, if a husband and wife are both on a credit card account, their plastic cards will have the same PAN. Therefore, if the husband mistakenly purchases the wrong item, the wife can return the item with a receipt and her credit card because her card's PAN will match that on the receipt: the PANs for multiple cards on the same account are the same. With tokenization, however, the husband and wife will each have separate and unassociated tokens, and the wife will be unable to return her husband's misguided purchase. Indeed, some manufacturers like Apple have device-specific tokens, meaning that a receipt from an ApplePay purchase using an iPad would not correspond to an ApplePay purchase made with an iPhone. Likewise, some token service providers (such as American Express) provide domain-specific tokens, so an NFC payment would have a different token than a Chip transaction.[112] While some merchants have work-arounds, such as additional loyalty card data that can provide an alternative method of identifying the customer, not all do, and maintaining such a program can be costly.

Likewise, the ability to see PANs lets merchants track customers' purchase histories. This can be used for advertising and loyalty programs, as well as for product safety recalls, fraud prevention, and anti–money laundering compliance. If a merchant sees that a customer has been purchasing baby products, for example, the merchant may want to send the customer targeted advertisements about other baby products or coupons for such products. By creating a

112 *See generally American Express Token Service*, *supra* note 40.

transactional history trail, payment card transactions provide merchants with a form of value that cash transactions do not. Similarly, if a merchant sees an attempted purchase that is inconsistent with a past transaction history in terms of location, amount, or item, it may raise red flags about potential fraud. And the ability to track multiple purchases enables merchants to spot suspicious purchase patterns (such as repeat mass purchases of stored value cards) for which anti–money laundering law requires suspicious activity reports.[113]

EMVCo has developed a specification for a Payment Account Reference (PAR), a twenty-nine digit alphanumeric sequence that would be consistent for an account regardless of form factor, but which could not itself be used to authorize payment.[114] Use of PARs, however, is potentially expensive. First, merchants must adapt their systems to handle these twenty-nine digit sequences. This can involve reprogramming thousands of point-of-sale terminals, which can in turn necessitate recertification of those terminals. Moreover, the PAR would be supplied by the token service provider—Visa, MasterCard, or AmEx. The U.S. PIN-debit networks are not certified as token providers by EMV and thus cannot provide PARs. Token service provider control over the PARs means that the providers could charge for PARs, thereby increasing merchants' cost of accepting payments. Ironically, then, while tokenization might decrease payment fraud rates, it could result in *higher* costs to merchants.

c. *Tender Choice and Payment Routing*

Digital wallets can affect both tender choice and payment routing. Tender choice refers to the type of payment the consumer chooses to use, such as credit, debit, or ACH. To the extent that digital wallets affect tender choice, it could result in a generational shift in tender overall given millennials' high use of mobile devices.

Tender choice is often determined by the very setup of a digital wallet. Some digital wallets, such as those offered directly by individual banks, allow only that bank's cards to be used. Thus Capital One Wallet (using Android host-card emulation) and ChasePay (using QR codes) allow the use of only Capital One and Chase cards, respectively.

Other digital wallets are open to cards from multiple financial institutions, but that does not necessarily translate to a diversity of cards in the wallet, much less active competition for transactions. While consumers might carry multiple cards in a physical wallet, they will frequently load only

113 *See, e.g.*, 31 U.S.C. § 5318(g)(1) (2012); 31 C.F.R. § 1020.320 (2017).

114 EMVCo, LLC, PAYMENT ACCOUNT REFERENCE (Jan. 2016), https://www.emvco.com/terms-of-use/?u=wp-content/uploads/documents/SB-167_Payment_Account_Reference_PAR_20160129015654268.pdf [https://perma.cc/7VEZ-JWRJ] (defining PAR as a "non-financial reference . . . [with a] fixed length 29 character data format").

a single card onto a digital wallet. The "top of the wallet" card is often the only card on a digital wallet. In this sense, digital wallets are often less "wallets" than simply digital versions of a single plastic card.

Because many consumers load only a single card onto a digital wallet, to the extent that consumers can be steered to loading a particular card onto the wallet, it effectively steers the consumer's choice of tender. Some digital wallets, like ApplePay and SamsungPay, were rolled out initially with participation by only credit card issuers. As a result, the first cards loaded on these wallets—and therefore the default card for the payments from the wallet absent additional consumer action—were credit cards. The result is a tender shift toward credit, and away from debit, at least for early adopters of these wallets.

Intellectual property rights may also affect tender and routing steering for digital wallets. For example, mobile wallets based on smartphones, like ApplePay and SamsungPay, offer consumers the option to authorize individual payments using biometrics—specifically, fingerprint scans. The use of a biometric for authorization is (in theory) quicker, easier, and more secure than having to enter a PIN number. Biometric authorization, however, is available only for credit and signature-debit cards; it is not available for PIN-debit cards. This is because when EMVCo, the joint venture between the major credit card networks, licensed the Common Payment Application—EMV's chip card specification—to U.S. debit Card Networks, the license did not include biometric Customer Verification Method (CVM). Thus ApplePay's default biometric CVM is not enabled for PIN-debit networks. This discourages use of PIN-debit and encourages use of credit or signature-debit.

Digital wallets may also affect routing choices. Routing refers to the processing of a transaction, and it can have a major effect on cost. A debit transaction that is routed through a signature-debit network is much more expensive for a merchant than if it were routed through a PIN-debit network.[115]

Additionally, there is differential ease of use for different types of payments with digital wallets. The differential ease of use can result either from the economic deals of digital wallet providers or from intellectual property rights limitations. Digital wallet providers can have an incentive to steer payment toward certain payment card networks' products or even toward certain banks' cards as part of their own economic deals, although to date this has not manifested itself.

115 *See Average Debit Card Interchange Fee by Payment card network*, BOARD GOVERNORS FED. RES. SYS. (July 14, 2017), https://www.federalreserve.gov/paymentsystems/regii-average-interchange-fee.htm [https://perma.cc/TRR4-TR83] (listing the average dual-message (signature-debit) interchange fee as 0.89% of average transaction values, compared to 0.64% of average transaction value for single-message (PIN debit) networks).

The combination of digital wallets and Chip technology also facilitates issuer steering of routing choices for debit card transactions. The Durbin Amendment requires that all debit cards have the possibility of being routed over two unaffiliated networks,[116] and that merchants be allowed to determine the routing of the transaction.[117] For magnetic stripe transactions, merchants are able to choose the routing based on the bank identification number on the card. For domestic Chip transactions, the routing selection is done through the AID software on the merchant's point-of-sale Chip terminal. The AID selects between different routing applications on the Chip card's chip. Not all routing applications contain the same routing choices. For example, MasterCard and Visa each have a "Common AID" for U.S. domestic transactions that contains all domestic PIN and signature-debit networks.[118] Additionally, MasterCard and Visa have their own AIDs, that contain, respectively, only MasterCard (and its Maestro PIN-debit subsidiary)[119] and Visa (and its Interlink PIN-debit subsidiary) networks.[120]

The use of a mobile wallet potentially enables the cardholder to override the Common AID in favor of the MasterCard AID or Visa AID (which do not contain unaffiliated PIN-debit networks), thereby undermining merchants' ability to choose the transaction routing. The override would work similar to the traditional magnetic stripe debit routing choice of pressing "credit" (for signature-debit) or "debit" (for PIN-debit). The cardholder can, in turn, be encouraged by an issuer or Card Network to exercise the override either by direct financial incentives, such as rewards for transactions run over particular network or by more subtle cues, such as the placement of AID choices on the device screen or the names assigned to the choices.

For example, a mobile wallet might ask the consumer if she wants to pay with "Visa debit" or "U.S. debit." The consumer knows that she has a Visa card because of the Visa logo on the front of the card. She likely does not know that her Visa card is also a card capable of running on one or more unaffiliated

116 *See* 15 U.S.C. § 16930-2(b)(1)(A) (2012) ("[A]n issuer . . . shall not . . . restrict the number of payment card networks on which an electric debit transaction may be processed to 1 such network; or 2 or more . . . [affiliated] networks."). For Durbin Amendment purposes, the "debit card" refers to the individual account, not the digital wallet application. Debit Card Interchange Fees and Routing, 76 Fed. Reg. 43,394, 43,409 (July 20, 2011) ("The entire virtual wallet is not considered to be the card . . . .").

117 § 16930-2(b)(1)(B) ("[A]n issuer . . . shall not . . . inhibit the ability of any person who accepts debit cards for payments to direct the routing of electronic debit transactions for processing over any payment card network that may process such transactions.").

118 *See* SHAZAM, EMV (June 2014), https://www.shazam.net/pdf/EMVUpdate_June2014.pdf [https://perma.cc/H4UP] (explaining that a common AID "helps the terminal and card 'talk' to each other" in domestic EMV transactions and the global AID "helps the terminal and card 'talk' to each other" in international EMV transactions).

119 *See* MASTERCARD ADVISORS, MERCHANT ADVISORY GROUP EMV WORKSHOP 18 (2014), http://www.merchantadvisorygroup.org/docs/default-source/2014-mid-year-conference/mag-emv-workshop-2014-0211-final.pdf [https://perma.cc/SSTF-SYQM].

120 *See* VISA TRANSACTION ACCEPTANCE DEVICE GUIDE, *supra* note 37, at 211.

PIN-debit networks. At best, these networks' logos will appear on the back of the card, but none are called "U.S. debit," which is a generic moniker for PIN-debit networks. When faced with the choice between the known brand and the unknown brand, the consumer is likely to choose the known brand, resulting in the payment being routed as a more expensive Visa signature-debit transaction.

This issue has already appeared on Chip terminals at point-of-sale, where a screen appears for the cardholder to "select payment." Merchants can reprogram their Chip terminals to turn off this selection screen, but doing so may necessitate EMV compliance recertification and leave the merchant exposed to counterfeit fraud liability under the EMV liability shift rule in the interim. Only the very largest and most sophisticated merchants are likely to attempt to reprogram their Chip terminals. With a mobile wallet, however, reprogramming is not an option for the merchant. The routing override may well be a violation of the Durbin Amendment and rules thereunder, but to the extent it occurs on mobile wallets, it will be more difficult for merchants to identify and address.

d. *Fraud and Data Security*

Digital wallets pose fraud and data-security breach risks for merchants. Payment card fraud and data security breaches are injurious to merchants in numerous ways. First, merchants lose the value of the goods and services they part with to the fraudster. Second, they lose the costs of restocking and of dealing with the fraud administratively. Third, they may suffer reputational damage vis-à-vis the consumers whose accounts were used for unauthorized transactions. Fourth, merchants may face liability to consumers related to the fraud. Fifth, if a breach results in fraud for *other* merchants, the breached merchant might be liable for the losses. And sixth, merchants pay merchant discount fees even on the fraudulent transactions. Merchant discount fees are sometimes refunded in certain cases with unauthorized transactions involving mobile wallets, but the inability to identify which transactions were undertaken with which form-factor means that merchants are unable to verify that they have been properly credited with reversals of merchant discount fees.

Different technologies present different security risks, and even within a technology, different form factors or devices may pose different security risks. Some digital wallets may be more vulnerable to use by fraudsters, who will load fake or unauthorized accounts onto digital wallets. This was a significant problem with ApplePay's initial rollout.[121] Moreover, the security of communications between a digital wallet and a merchant may vary by device. To the extent that there is a data security breach in the communications

121 *See* Andrew Ross Sorkin, *Pointing Fingers in Apple Pay Fraud*, N.Y. TIMES (Mar. 16, 2015), https://www.nytimes.com/2015/03/17/business/banks-find-fraud-abounds-in-apple-pay.html [https://perma.cc/WQ5u-X7MD].

process, the stolen data can itself be used for unauthorized transactions. Even if the unauthorized transactions occur at other merchants, there can still be serious reputational harm to the breached merchants, which might also have liability to other merchants and consumers.

The Honor All Wallets rules and lack of ability to identify devices means that merchants cannot protect themselves either proactively or reactively by declining to accept certain devices or by limiting the types of purchases they will allow on a device. For example, even if a merchant were to believe that communications via certain NFC wearables were compromisable, the merchant could not refuse to accept NFC payments from those wearables.

Likewise, if a security problem were to emerge with specific wallets, allowing them to be used for fraudulent transactions, merchants could not protect themselves reactively by limiting purchases of open-loop gift cards (a favorite purchase for fraudsters) or of high-value items with ApplePay. The Honor All Wallets rules prevent merchants from refusing to accept or from discriminating against less secure devices despite the risks they pose to merchants.

e. *Intellectual Property Liability*

Patent trolls are a fact of modern business life. Patent trolls are firms that purchase patents for the purpose of bringing litigation against alleged infringers of the patents. As a result, patent trolls will often sue indiscriminately any party that has had any interaction with a patent.

Mobile wallets involve new (and changing) technologies that can implicate a range of patents. As a result, they are a fertile ground for patent trolling. While merchants are generally involved in mobile wallets only as recipients of payments (or potentially as users in the case of chargebacks and returns), large merchants make tempting targets for patent trolls. Indeed, some of the merchants interviewed for this Article have been sued for patent infringement on the basis of their acceptance of contactless payments.

Because merchants have no ability to determine exactly what technology—and thus what patents—are implicated by a particular payment's communication medium, they have little ability to protect themselves against potential patent infringement liability other than by negotiating for indemnification from their acquirer banks. The acquirer banks themselves, however, do not have control over which technologies are allowed to access a payment card network. That decision is controlled solely by the Card Network itself.

Standard law-and-economics theory dictates that liability should be placed on the party with the lowest cost to avoid a harm, the so-called "least-cost

avoider."[122] In the case of patent liability for mobile wallets, the only party with the ability to avoid the harm of patent infringement is the Card Network because it is the party that makes the decision whether to allow technology to access the network. Placing the liability on the least-cost avoider would suggest that the Card Networks should completely indemnify merchants for any patent infringement liability caused by accepting a device approved by the network. The fact that merchants are not completely indemnified by the Card Networks means that the Card Networks do not internalize the full cost of patent infringement, so they are not incentivized to take the optimal level of care when approving technologies for accessing the network. Accordingly, accepting payments from mobile wallets creates a risk of patent infringement liability for merchants.

f. *Cost of Accepting Payments*

Beyond tender and routing choices, digital wallets raise the possibility of potential increases in the costs of accepting payment. The addition of digital wallet providers into the payment ecosystem means that there are additional mouths at the table. Digital wallet providers expect to be compensated for their services, and this compensation must come from somewhere. Apple, for example, reportedly receives fifteen basis points on every ApplePay transaction.[123] These fifteen basis points are paid by the card issuer, which reduces the issuer's profits. As ApplePay's transaction volume grows, these fifteen basis points will become increasingly significant to issuers, who will be incentivized to recover them from other parties, such as by pressuring the Card Networks to increase interchange fees.

The Card Networks, too, may look at digital wallets as a revenue source. Thus Visa created a "tokenization" fee, reportedly seven cents per token and two cents per decline, which it waived for the first year,[124] before later suspending the fee for issuers that do their processing through Visa.[125] It would not be surprising if Visa were to reinstitute the fees once issuers have sufficiently committed—and become locked into—tokenization.

Similarly, MasterCard has created "digital enablement fees" for both issuers and acquirers.[126] Issuers are subject to a 50-cent "digitization" fee for

122 *See, e.g.*, GUIDO CALABRESI, THE COSTS OF ACCIDENTS 136-38 (1970).

123 *See supra* note 57 and accompanying text.

124 *See VISA CEO Confirms Tokens as New Network Revenue Stream*, *supra* note 50 (noting that Visa "put a rate schedule out there for tokenization," though Visa waived tokenization fees for 2015).

125 *See* John Stewart, *With New Digital Program, Visa Drops Token Fees, Offers Issuers Single Connection to All Services*, DIGITAL TRANSACTIONS (June 2, 2015), http://www.digitaltransactions.net/with-new-digital-program-visa-drops-token-fees-offers-issuers-single-connection-to-all-services [https://perma.cc/QG2K-CHRU].

126 *See* Jim Daly, *As Card-Industry Use of Tokens Increases, MasterCard Plans "Digital Enablement" Fees*, DIGITAL TRANSACTIONS (Aug. 14, 2014), http://www.digitaltransactions.net/as-card-industry-use-of-tokens-increases-masterCard-plans-digital-enablement_-fees/ [https://perma.cc/JP54-SPZD].

the provision of a token and a "Digital Enablement Service Lifecycle Management" fee of 10 cents per month for a tokenized PAN, as well as a fee of 2.5 cents for calls to its "alternate network application programming interface."[127] Acquirers are charged one basis point on select card-not-present transaction volumes.[128]

Additionally, as discussed earlier in subsection II.B.2.b, the networks are likely to charge for PAR numbers that stand in for a PAN with a tokenized payment in order to facilitate fraud detection, returns, and loyalty programs. The PAR is necessary only because of tokenization, which many merchants do not want; through tokenization, the Card Networks are in a position to charge merchants more for a less valuable product.

When considering all of the risks posed by digital wallets, it is not clear if there is a compelling general value proposition for their acceptance by merchants. On the one hand, digital wallets offer the possibility of better data security and integration of loyalty programs with payments. On the other hand, they pose the specter of loss of data through tokenization, loss of control over customer data and the customer relationship, undifferentiated security risks, greater liability, and higher costs of payment acceptance both because of tender and routing shifts and because of additional fees. The tradeoffs may vary by merchant and by digital wallet; it may well be that in some cases it makes sense for a merchant to accept a digital wallet. Because of the Honor All Wallets rules, however, merchants are not able to select which digital wallets they wish to accept and on what terms. The result is to preclude merchants from protecting their own interest or from seeking out favorable deals with individual digital wallet providers. Thus it does not even matter how compelling a business proposition a particular digital wallet offers to a merchant; the merchant will have to accept that digital wallet on the same terms as all other digital wallets if it accepts any payments that use that wallet's communications technology.

3. The Honor All Wallets Rules

At this point we have seen how there is a tremendous variety in digital wallet product design. Different digital wallets present different cost–benefit propositions to consumers and merchants. As discussed in subsection II.A.3, consumers have the ability to eschew use of digital wallets and to pick the particular wallet(s) they wish to use. This provides consumers with some (imperfect) measure of protection against riskier products.

For merchants, however, the range of costs and benefits across digital wallets is more problematic. Merchants lack the "just say no" option because

127 *Id.*
128 *Id.*

of the combination of creeping technology mandates and certain Card Network rules that limit their ability to selectively accept digital wallets.

Presently, merchant acceptance of digital wallets is limited. Virtually all merchants accept payments through only a limited number of technologies, either because they lack the equipment to accept other technologies or because they have not chosen to activate the equipment features that would accept other technologies.[129] Moreover, there is currently no mandate in the United States for merchants to accept payments through any particular type of technology. Yet signs point in this direction, including the imposition of Card Network technology mandates in Europe, Canada, and Australia.[130]

Even without technology mandates, however, there is no going backward in payment systems. Once a system is turned on, as a business matter, there's no turning it off. Turning off a payment system risks alienating customers and losing transactions from customers who have relied upon acceptance of their system or device. Moreover, NFC contactless technology in particular is rapidly becoming the new standard for in-person payments.[131] Given how important digital wallets are expected to be in twenty-first century retailing, and the significance of path dependence and first-mover advantages, the terms under which merchants end up accepting digital wallets will have an enormous effect on the shape of retailing and payments.

a. *The Honor All Wallets Rules*

If merchants were free to pick and choose which digital wallets they wished to accept or to condition their acceptance, then merchants could evaluate the basis on which they were willing to accept the costs imposed by any particular digital wallet. That, however, is not the situation merchants face today.

All of the Card Networks have network rules binding on their acquirer and issuer members.[132] Card Network rules are incorporated by reference in

129 For example, in mid-2016, only around two million of the thirteen million point-of-sale terminals in the United States were equipped to accept NFC payments. *See* Karen Webster, *UK's Lessons for U.S. Mobile Payments Adoption*, PYMNTS.COM (Mar. 21, 2016), https://www.pymnts.com/nfc/2016/uk-lessons-for-us-mobile-payments-adoption/ [https://perma.cc/MM3E-U358] (describing the number of terminals that can accept NFC payments). These terminals represent some 15% of terminals, but 21% of merchants. Press Release, Javelin Strategy, A Third of U.S. Retail Establishments to Accept Contactless Cards by 2019 in a Second Wave of EMV (Oct. 15, 2015), https://www.javelinstrategy.com/press-release/third-us-retail-establishments-accept-contactless-cards-2019-second-wave-emv [https://perma.cc/9NXA-5846].

130 *See* Webster, *supra* note 129.

131 The vast majority of new POS terminals in the U.S. and worldwide are NFC equipped. *See Merchants Worldwide Are Installing More Contactless Terminals—And Turning on NFC*, DIGITAL TRANSACTIONS (Feb. 17 2015), http://www.digitaltransactions.net/merchants-worldwide-are-installing-more-contactless-terminals-and-turning-on-ntc [https://perma.cc/V4PS-Y26S] (noting that 75% of new POS terminals in the U.S. in 2014 were NFC capable); *see also* Press Release, Javelin Strategy, *supra* note 129.

132 *See* Levitin, *supra* note 9, at 1324.

merchant contracts. For example, Visa requires that acquirers have a merchant agreement with every merchant that takes Visa cards.[133] The merchant agreement must include language requiring the merchant to comply with all the Visa Rules, including those regarding acceptance.[134] Thus, even though merchants may lack direct contractual dealings with Visa, they are nonetheless bound by its rules.

Among these rules are the "Honor All Cards" rules requiring merchants to accept all cards carrying the Card Network's logo.[135] The Card Networks interpret their Honor All Cards rules to be "Honor All Wallets" rules, meaning that merchants are required to accept all devices set up to transact through the Card Network if the merchant accepts payments using the communications technology employed by the device.[136] For example, Visa's Honor All Cards rule mandates that any "U.S. Merchant that wishes to accept Visa Cards must accept any valid Visa Card in its category of acceptance that a Cardholder properly presents for payment."[137] A "Visa Card" is defined for

133 VISA CORE RULES, *supra* note 26, § 1.5.2.1 ("An Acquirer must have a Merchant Agreement with each of its Merchants to accept Visa Cards.").

134 *See id.* ("The Merchant Agreement must include language that requires the Merchant to do all of the following[:] . . . Comply with the Visa Rules regarding use of the Visa-Owned Marks, Visa acceptance, risk management, Transaction processing, and any Visa products, programs, or services in which the Merchant is required to, or chooses to, participate . . . ."). For an equivalent requirement imposed by MasterCard, see MASTERCARD, MASTERCARD RULES § 5.1.2 (2017), which specifies "[e]ach Merchant Agreement must contain the substance of each of the Standards set forth in Rules 5.4 through 5.13 [including the Honor All Cards Rule in § 5.8.1], and any other Standards applicable to the nature and manner of the Merchant's business."

135 Since a 2003 litigation settlement, there has been a carveout from the MasterCard and Visa Honor All Cards rules allowing merchants to choose whether to accept only their credit products, only their signature-debit products, or both. Within each category of cards accepted, however, the Honor All Cards rule still applies.

136 It is unclear how the Honor All Wallets rules operate when there is an intermediate payment aggregator, such as PayPal or Square. In the payment aggregator model, the aggregator pays the merchant using a low-cost payment method, such ACH, and in turn bills the Card Network as if it were the merchant. The aggregator business model is based on arbitraging the difference in merchant discount fees paid by the aggregator and the merchant. Presumably a merchant that accepts PayPal mobile payments via QR technology is not obligated to accept other QR devices because the merchant has not actually received a payment from a Card Network directly. *Cf.* Levitin, *Payment Wars*, *supra* note 11, at 479-81. *See generally Becoming a Payment Facilitator, Payment Service Provider [PSP] or Payment Aggregator*, AGILE PAYMENTS, https://www.agilepayments.com/downloads/payfac.pdf [https://perma.cc/CXT8-HVMH].

137 VISA CORE RULES, *supra* note 26, § 1.5.4.5. Similarly, MasterCard requires "Merchants that choose to accept . . . MasterCard Cards [to] honor all . . . MasterCard Cards without discrimination when properly presented for payment." MASTERCARD, *supra* note 134, § 5.8.1. MasterCard also expressly provides that unless otherwise stated, its rules regarding card acceptance also apply to non-card access devices. *Id.* at 257. American Express likewise requires merchants to "accept the Card as payment for goods and services . . . sold . . . at all of your Establishments, except as expressly permitted by Applicable Law." AMERICAN EXPRESS, AMERICAN EXPRESS MERCHANT REFERENCE GUIDE § 3.1 (Oct. 2017), https://icm.aezp-state.com/internet/NGMS/US_en/Images/merchantpolicypdfs/US_RefGuide_NS.pdf [https://perma.cc/A45K-HASZ]. American Express defines "card" to mean "[a]ny card, account access device, or payment device or service bearing our or our Affiliates' Marks and issued by an Issuer or a Card Number." *Id.* at 55.

the U.S. region as "[A Magnetic Stripe and/or a Visa Contactless Payment Device] bear[ing] the Visa Brand Mark that enables a Visa Cardholder to obtain goods, services, or cash from a Visa Merchant or an Acquirer."[138] Based on this definition, Visa's attorney at a 2013 class action settlement fairness hearing represented that "the Master Card and Visa Honor-all-Cards Rules apply to both cards but also to other devices including contactless devices."[139]

Similarly, MasterCard requires "Merchants that choose to accept . . . MasterCard Cards [to] honor all . . . MasterCard Cards without discrimination when properly presented for payment."[140] MasterCard also expressly provides that unless otherwise stated, its rules regarding card acceptance apply to non-card access devices.[141]

American Express likewise requires that "[m]erchants must accept the Card as payment for goods and service . . . sold . . . at all of your Establishments, except as expressly permitted by Applicable Law."[142]

The Honor All Wallets rules tie acceptance of traditional plastic-based card payments with acceptance of non-card devices that utilize the same communications technology. If a merchant accepts a Card Network brand payments using a given type of communications technology—magnetic stripe, NFC, QR code, etc.—the merchant must accept the Card Network brand payments from all devices using that technology. A merchant may not accept only certain devices using a technology. Thus if a merchant is willing to accept magnetic stripe payments, it must also accept emulated magnetic stripe payments, such as those used by SamsungPay.[143] Likewise, if a merchant is willing to take payment through NFC, for example, the merchant must accept all network-approved NFC payment devices, such as ApplePay and Google Pay.[144]

---

138 VISA CORE RULES, *supra* note 26, at 793.

139 Transcript of Fairness Hearing at 38, *In re* Payment Card Interchange Fee and Merchant Discount Antitrust Litigation, MDL No. 1720 (E.D.N.Y. Sept. 12, 2013).

140 MASTERCARD, *supra* note 134, § 5.8.1.

141 *Id.* at 257.

142 AMERICAN EXPRESS, *supra* note 137, § 3.1.

143 Emulated magnetic strip payments, also known as magnetic secure transmission, send a magnetic signal from a device to a nearby card reader that emulates swiping a physical card with additional security. *See What is MST? (Magnetic Secure Transmission)*, SAMSUNG, http://www.samsung.com/us/support/answer/ANS00043865/ [https://perma.cc/VD9C-4R5B].

144 Many U.S. merchants that invested in accepting contactless NFC payments did so before ApplePay was released in October 2014, at a time when NFC payments were made almost exclusively through traditional plastic cards with NFC RFID chips in them rather than through digital wallets using NFC technology. *See* Matt Hemblen, *Despite Apple, NFC Is Catching On—Just Not for Payments Quite Yet*, COMPUTERWORLD (Dec. 19, 2012, 6:00 AM), https://www.computerworld.com/article/2493828/mobile-payments/despite-apple-nfc-is-catching-on-just-not-for-payments-quite-yet.html [https://perma.cc/K4ZX-NUYX]. The Honor All Wallets rules, along with the rise of NFC digital wallets, may change the implications of these merchants' investments.

The Honor All Wallets rules not only require acceptance of all wallets using a certain technology, but also nondiscrimination among devices and among technologies. Therefore a merchant who takes magnetic stripe payments must accept emulated magnetic stripe payments, such as those used by SamsungPay, *without discrimination*. Similarly a merchant that takes NFC cards must accept all NFC devices, including devices running ApplePay and Google Pay wallets, *without discrimination*.

The inability to discriminate on terms of acceptance not only means that merchants cannot price for the risks imposed by particular wallets, but also impedes merchants' ability to partner with wallet providers. A merchant might want to partner with a particular digital wallet provider to gain access to the wallet as a platform for advertising and loyalty programs. The Honor All Wallets rules would permit such a partnership, but the merchant could not discriminate in favor of its partner to encourage use of its wallet. As a result, merchants' incentive to partner with a particular digital wallet provider is reduced; they are instead incentivized to partner with the Card Network itself to gain access to all wallets.

Currently, U.S. merchants are not mandated to accept payments using any particular technology. This situation may well change, however. Since 2014, contactless payment acceptance has been required in Australia and for all new and upgraded point-of-sale terminals in Canada.[145] Furthermore, MasterCard has mandated that all card-present merchants in Europe accept contactless payments with NFC technology by 2020,[146] and Visa has issued a contactless acceptance mandate for the U.K. by 2020.[147] It would seem, then, only a matter of time before there is a contactless mandate in the U.S.[148]

In the U.S., Visa has given indications that it considers magnetic stripe technology a legacy system that will be phased out as new cards and new contactless readers are required to support not only the magnetic stripe data

145 *See* SMART PAYMENT ASS'N, AN OVERVIEW OF CONTACTLESS PAYMENT ACCEPTANCE BENEFITS AND WORLDWIDE DEPLOYMENTS §§ 3.2–3.3 (2016), https://www.smartpaymentassociation.com/images/news/16-04-26-SPA-Contactless-Payment-Benefits-WP-Final.pdf [https://perma.cc/6CN5-TLQA].

146 *See* Press Release, MasterCard, MasterCard Fast Tracks Mobile Payment Acceptance in Europe Helping Europeans to Tap Everywhere by 2020 (Sept. 10, 2014), http://newsroom.mastercard.com/press-releases/mastercard-fast-tracks-mobile-payment-acceptance-europe-helping-europeans-tap-everywhere-2020/ [https://perma.cc/5AQN-8E5Q].

147 *See* Press Release, Visa, The Contactless Transaction Threshold Increases to £30 Today. Visa Europe Welcomes This New Threshold Increase and Believes It Will Be the Most Significant to Date (Jan. 9, 2015), https://www.visa.co.uk/newsroom/the-contactless-transaction-threshold-increases-to-ps30-today-visa-europe-welcomes-this-new-threshold-increase-and-believes-it-will-be-the-most-1241648 [https://perma.cc/MK5B-AM9U].

148 A similar pattern of rollouts can be observed with the adoption of EMV, with the U.S. being the last region to adopt the technology. *See* Tina Orem, *Global EMV Adoption Leaps; U.S. Still Lags*, CREDIT UNION TIMES (Jan. 5, 2017), http://www.cutimes.com/2017/01/05/global-emv-adoption-leaps-us-still-lags [https://perma.cc/8U5J-SBE4].

interface, but also contactless chip functionality.[149] Moreover, the majority of new point-of-sale terminals in the United States are now shipped with NFC capability.[150] U.S. merchants may well find themselves required to accept NFC payments in the near future, and thus to accept all NFC wallets.

b. *Problems Identifying Digital Wallets*

Even without the Honor All Wallets rules, merchants would have limited ability to accept digital wallets selectively because they cannot identify the particular digital wallet used or even if a digital wallet is being used. When a consumer pays with a digital wallet based on a smartphone using NFC communication, for example, the merchant cannot determine whether an NFC-enabled card or an NFC-enabled digital wallet was used, much less which wallet on the smartphone was used. Likewise, because of magnetic stripe emulation technology merchants cannot tell if SamsungPay or a traditional magnetic swipe card has been used for a transaction absent physical observation. While such observation is possible for some merchants, it is not possible for others, including those with self-service kiosks or even those with registers where the consumer is the party to handle the point-of-sale terminal.

Although Card Networks have typically required card issuers to provide a "Form Factor Indicator," "device type value," or other form of offline data authentication to identify the device being used to make the transaction,[151] merchants interviewed for this Article uniformly claim that card issuers are not in fact providing form factor information, despite the presence of a data field for such information. As a result, merchants do not even know with which digital wallets they are dealing.

All in all, then, merchants are not able to identify digital wallets, but even if they could, they would still be prohibited from selective or conditional acceptance of digital wallets that use a particular communications technology through which they already accept payments made on a Card Network brand. A merchant cannot decide to take one type of digital wallet, but not another, if the wallets use the same basic communications technology, even if the risks

149 *See* VISA TRANSACTION ACCEPTANCE DEVICE GUIDE, *supra* note 37, at 240.

150 *See* Stewart, *supra* note 125 (noting that 75% of new POS terminals shipped in 2014 were NFC capable).

151 *See, e.g.*, MASTERCARD, *supra* note 134, at 203 ("An Issuer must ensure that each contactless-enabled MasterCard Card or Access Device newly issued or re-issued on or after 18 October 2013 is personalized with the appropriate device type value."); VISA CORE RULES, *supra* note 26, § 4.1.22.10 ("All contactless chip cards issued on or after 1 October 2015 must support offline data authentication."). Visa's technical standard for offline data authentication, VCPS 2.1, includes a form factor indicator. *See* VISA TRANSACTION ACCEPTANCE DEVICE GUIDE, *supra* note 37. The form factor indicator must be sent to Visa by the Acquirer if present in the card. *See* VISA, VISA SMART DEBIT/CREDIT AND VISA PAYWAVE 126 (2016), https://www.visa.com/chip/merchants/grow-your-business/payment-technologies/credit-card-chip/docs/visa-emv-merchant-aig.pdf [https://perma.cc/55B3-53FE].

involved in different wallets vary materially. In other words, the Honor All Wallets rules tie acceptance of different types of payment devices using the same basic communications technology. Acceptance of traditional magnetic stripe transactions is tied to acceptance of digital wallets using magnetic stripe emulation; acceptance of NFC transactions from plastic cards is tied to acceptance of NFC transactions from various digital wallets; acceptance of Internet transactions is tied to acceptance of digital wallets using Internet communication; and acceptance of one digital wallet using a communications technology is tied to the acceptance of all digital wallets using that technology.

c. *Antitrust Implications of the Honor All Wallets Rules*

The Honor All Wallets rules raise credible antitrust concerns about illegal restraint of trade.[152] The Honor All Wallets rules restrict merchants' ability to accept digital wallets selectively or conditionally. This enables the Card Networks to maintain their market power in the overall payment card market in the face of technological transformation. Absent the Honor All Wallets rules' restraint on merchants, more digital wallets would compete by offering cheaper payments using PIN-debit and ACH.

The Honor All Wallets rules also operate as a type of tying arrangement that ties together plastic cards and digital wallets and thereby also ties the markets in the related products of plastic Card Network services and digital wallet network services. This tying enables the Card Networks to expand their market share in the digital wallet network services area, particularly as token service providers. Accordingly, the Honor All Wallets rules should invite serious scrutiny by competition regulators and could presage private litigation.

d. *From Honor All Cards to Honor All Wallets*

The Honor All Wallets rules are an expanded interpretation of the Card Networks' Honor All Cards rules. The traditional Honor All Cards rules required merchants to accept all types of cards—credit and debit, rewards and non-rewards, co-brands and non-co-brands—from all issuers.[153] And for traditional credit card transactions, variation among issuers is immaterial to merchants: all issuers (and acquirers) are FDIC-insured financial institutions, and the payments from the

152 An assumption of this analysis is that there is no collusion between the Card Networks; such collusion would raise different and additional antitrust issues. Likewise, a consideration of the antitrust issues presented by the EMVCo LLC joint venture and of its reported limited licensing of its tokenization specification is beyond the scope of this Article.

153 *See In re* Visa Check/MasterMoney Antitrust Litig., 192 F.R.D. 68, 73 (E.D.N.Y. 2000).

issuers to the acquirer are guaranteed by the Card Network.[154] Merchants, therefore, have no reason to price differentially solely on the basis of card issuer (other than differences in chargeback policy by issuers).

Variations in type of card, however, present a different set of concerns for merchants than do variations in issuer. The Honor All Cards rules effectively tie acceptance of one type of card with acceptance of other types of cards. This is a problem for merchants because different types of cards entail different costs and risks. For example, rewards cards bear higher interchange fees than non-rewards cards. These higher interchange fees get passed along to merchants in their merchant discount fee, yet merchants see no marginal benefit from accepting rewards cards.[155] Because the Honor All Cards rules require merchants to accept all of these cards on the same terms, merchants cannot discriminate between high-cost and low-cost cards.

The Honor All Cards rules also historically tied acceptance of the Card Networks' credit cards to the acceptance of the Card Networks' signature-debit cards.[156] Signature-debit cards—cards for which transactions are authorized by a signature rather than a PIN—have higher interchange fees than PIN-debit cards and are inherently less secure, increasing chargeback risk for merchants.[157] The Honor All Cards rules, however, required merchants to accept the more expensive and less secure signature-debit cards as a condition of taking credit card payments, enabling entry into the payments market by an inferior product at the expense of the PIN-debit products.

The Honor All Cards rules have been the subject of two rounds of major antitrust litigation that have resulted in some of the largest private litigation settlements in history. The first round of the litigation, dealing with the tying of credit and signature-debit cards by MasterCard and Visa, resulted in a $3.05 billion class action settlement (and numerous private settlements by class opt-outs) and a temporary relaxation of the rule to allow merchants to accept credit cards without accepting signature-debit cards.[158] The second round of litigation focused on the tying of rewards cards with non-rewards cards (a tying bolstered by certain other

154 *See* VISA, VISA INTERNATIONAL OPERATING REGULATIONS 604 (2013), https://usa.visa.com/dam/VCOM/download/merchants/visa-international-operating-regulations-main.pdf [https://perma.cc/SF6A-2HD7].

155 *See* Levitin, *supra* note 9, at 1391 ("If the honor-all-cards rule was eliminated, merchants would likely refuse to accept cards that had high interchange fees (and hence high merchant discount fees).").

156 *See In re* Visa Check/Mastermoney Antitrust Litig., 280 F.3d 124, 131 (2d Cir. 2001) ("Defendants have an 'honor all cards' policy, which requires any merchant accepting any of their credit cards to accept all of their payment cards.").

157 *See* Levitin, *supra* note 9, at 1323 tbl.1 (illustrating that signature-debit cards cost U.S. retailers more per transaction on average than do PIN-debit cards). The inherent security limitations on signature debit cards are apparent in that they do not allow for cash back at point-of-sale; there is no such thing as a signature ATM card.

158 *See In re* Visa Check/Mastermoney Antitrust Litig., 297 F. Supp. 2d 503, 507-508 (E.D.N.Y. 2003).

Card Network rules). It initially resulted in a $7.25 billion class action settlement that was then thrown out on appeal.[159] Critically, although the proposed settlement would have allowed merchants to surcharge for cards in some situations, it would not have affected the Honor All Cards rules and would have in fact permanently enjoined all merchants (including those not yet in existence) from challenging the rule.[160]

The Honor All Wallets rules are formally interpretations of the Honor All Cards rules. Functionally, however, they are new restraints that enable the Card Networks to maintain their power in the credit and debit card markets, both in terms of card acceptance for merchants and of market power over issuing banks and consumers as technological advances move the market into digital wallets. As such, the transformation of the Honor All Cards rules into Honor All Wallets rules raises the same fundamental problems that existed in past applications of the Honor All Cards rules.

At the same time, however, the Honor All Wallets rules do more than the Honor All Cards rule. The Honor All Cards rules were an *intra*brand restriction: they required a merchant that accepted one Visa card to accept them all. The Honor All Wallets rules, however, function as an *inter*brand restriction: if a merchant accepts Visa contactless cards, the merchant must also accept all Visa payments on all NFC devices. That means that the merchant cannot elect to accept only MasterCard NFC (or PIN-debit, or ACH) payments from mobile wallets. Because a digital wallet can contain multiple brands' cards, the Honor All Wallets rules function as an interbrand restriction, not merely an intrabrand restriction. This difference is significant, because—as explained in the next subsection—antitrust law is much more skeptical of interbrand restrictions than intrabrand restrictions.

e. *Harms to Competition*

Antitrust law is about protecting competition, not competitors. Therefore, antitrust violations require injuries to competition. Although the Honor All Wallets rules restrict merchants' ability to bargain for the terms under which they accept payments and effectively impose significant risks and costs on merchants, those consequences do not amount to an injury to competition and thus do not establish grounds for antitrust liability. The Honor All Wallets rules *do*, however, injure competition by restricting competition for network services at point-of-sale (as opposed to online). This has the effect of foreclosing the entry of digital wallets utilizing lower-cost point-of-sale payment methods, such as PIN-debit and ACH payments. Not only does this foreclosure harm competing digital

159 *See In re* Payment Card Interchange Fee & Merch. Disc. Antitrust Litig., 986 F. Supp. 2d 207, 217 (E.D.N.Y. 2013), *rev'd*, 827 F.3d 223 (2d Cir. 2016).

160 *See In re Payment Card Interchange Fee*, 827 F.3d at 238-39.

wallets, but it also harms merchants by forcing them to deal with a market in which prices are artificially inflated because of reduced competition.

Absent the Honor All Wallets rules, it is not clear that there would be a market for open digital wallets that make payments from the Card Networks' credit and signature-debit accounts. Consumers will only use such digital wallets if merchants accept them. Merchants, however, have little reason to accept Card Network payments through digital wallets. Merchants face additional costs for accepting digital wallets, including potential loss of customer data, additional fees, and various security (and litigation) risks. Digital wallets do not generally offer sufficiently offsetting benefits, particularly because all consumers with digital wallets also have plastic payment cards (and are usually carrying them). Merchants are thus unlikely to lose many sales by not accepting digital wallet payments. Moreover, unlike the shift from cash to plastic cards, the shift from plastic cards to digital wallets does not enable greater consumer consumption and therefore merchant sales. Instead, there would be only additional value to a merchant from accepting a Card Network payment on a digital wallet if the merchant partnered with the digital wallet provider to gain access to the digital wallet as an advertising and loyalty program platform.

Open digital wallets, however, need not make Card Network payments. Instead, they can make payments using low-cost payment systems like ACH or PIN-debit cards, such as with staged wallets like PayPal. ACH is a very low-cost payment system that is not associated with any device; it is often used for direct deposit and automatic bill pay. ACH payments merely require transmission of the payor and payee's bank account and routing numbers and the payment amount to the payor or payee's financial institutions.

A digital wallet can make ACH a much more consumer-friendly payment system. Instead of having to remember a sequence of disembodied bank account and routing numbers, a consumer can enter that information into a digital wallet once and then use that digital wallet much like a debit card.

Likewise, a digital wallet can be used to make PIN debit card payments. While PIN debit card transactions are more expensive for merchants than ACH transactions, they are much cheaper than transactions on both the Card Networks' signature debit cards and credit cards. Thus, absent the Honor All Wallets rules, one would expect to see merchants accepting digital wallets selectively and on a bargained-for basis, with digital wallets that offer ACH or PIN-debit payments having a substantial advantage because of the lower cost of those payments.

The Honor All Wallets rules get the Card Networks around the problem that merchants are not generally attracted to digital wallets that use their cards. The Honor All Wallets rules prevent merchants from being able to accept digital wallets selectively or conditionally if the merchant also takes plastic cards. A merchant might want to accept only ACH and PIN-debit payments

from digital wallets, but cannot under the Honor All Wallets rules. Instead, the merchant must also accept digital wallets that make payments on the Card Network's credit and signature-debit networks. Similarly, merchants might simply refuse to accept credit and signature debit–based digital wallets. But if a merchant accepts Visa's contactless NFC plastic cards, however, the merchant must also accept all Visa payments on NFC-based digital wallets. The merchant has no option of accepting only PIN-debit payments with digital wallets. The Honor All Wallets rules thus help the Card Networks gain entry to the digital wallet market despite offering noncompetitive products.

The Honor All Wallets rules do more, however, than help the Card Networks gain entry into the digital wallet market. Because of the unusual structure of payment systems, to the extent that a consumer adopts a digital wallet that uses the Card Network's cards, that consumer is unlikely to also use ACH or PIN debit digital wallets.

Payment systems are "two-sided" markets with two types of "consumers": payors (issuers and consumers) and payees (acquirers and merchants).[161] A payment system is of no value to payors if payees refuse to accept payments using the system, and to payees if payors refuse to make payments using the system. Instead, to make a two-sided market viable, there needs to be a threshold number of both types of "consumers." The two-sided nature of payment systems markets creates a "chicken-and-egg" problem for new systems—payors won't join the system unless enough payees accept it, and vice-versa.[162] The reason for this is that payment systems have strong "network effects," meaning that the value of participating in the system is increased (or decreased) by the number of other types of participants in the system. The more merchants accept a payment method, the more valuable the payment method is to consumers, and vice versa.[163]

Industries with network effects have natural barriers to entry. Moreover, to the extent that both payors and payees tend to use only one type of payment product, the adoption of one system operates to exclude other systems by making it impossible for other systems to surmount the network effects, because too many of the potential network participants are already committed to the first system. This is likely the case with device-based digital wallets. Whereas consumers may use multiple online digital wallets offered by various merchants, they are unlikely to load multiple general-purpose digital wallets onto mobile devices. Instead, consumers are likely to load and use a single general-purpose digital wallet, which may itself contain only one linked card. Therefore, to the

161 *See supra* notes 10–12 and accompanying text.

162 *See* Levitin, *supra* note 9, at 1365 (describing two-sided networks' chicken-and-egg problem "in which it is impossible to attract one type of customer without having first attracted the other").

163 *Id.* at 1364-65 ("[A] network's value to its participants depends on the network's size.").

extent that a consumer adopts a particular digital wallet, that consumer is not available for other digital wallets to overcome the "chicken and egg" problem.

The Honor All Wallets rules help the Card Networks swamp rival networks competing for access to digital wallets. The rules enable the Networks to gain entry to the digital wallet market because it ensures merchant acceptance, and thus consumer willingness to use wallets that use the Card Networks' cards. With entry achieved and their market share artificially increased, the Card Networks can then divert part of the higher fees merchants are charged on their payments to consumers in the form of rewards, incentivizing them to use the digital wallets with the Card Networks' cards, rather than digital wallets with PIN or ACH.

The situation is analogous to the Honor All Cards rules' tying of signature-debit acceptance to credit card acceptance. Signature-debit is a more expensive and riskier product than PIN-debit, and many merchants would have preferred to accept only PIN-debit products and credit cards, not signature-debit. But when merchants were forced to accept signature-debit as well as PIN-debit, signature-debit flourished because part of the higher interchange fees on the signature-debit were rebated back to consumers by the Card Networks and their issuers as "rewards" to encourage the use of the signature-debit product.[164] The Honor All Wallets rules work similarly to foreclose entry to digital wallets offering ACH and PIN-debit payments.[165]

---

164 *See also supra* notes 156–57 and accompanying text.

165 The Honor All Wallets rules may also have the ironic effect of foreclosing entry to digital wallets that use communications technology other than NFC; Honor All Wallets could, in fact, ultimately mean only "Honor Only NFC Wallets." The Honor All Wallets rules do not require the acceptance of any particular communications technology by merchants, only the acceptance of all devices using a communications channel the merchant already accepts. The adoption of the EMV liability shift rule has incentivized many merchants to invest in new EMV-capable point-of-sale terminals. *See supra* notes 44–46 and accompanying text. Virtually all EMV Chip terminals sold today come with the hardware capability of accepting Chip, magnetic stripe, and NFC payments. Moreover, for at least some manufacturers, the default setting is that all three communication channels are activated on installation. Although merchants can disable the NFC hardware, the mere fact that they already have the hardware means that the number of merchants that can readily accept NFC payments is greatly expanded, thereby surmounting part of the chicken-and-egg problem of technology acceptance in two-sided markets.

This expansion of NFC-equipped merchants may have the effect of foreclosing entry for mobile wallets that use other technologies, because the acquisition and certification of EMV Chip terminals can eat up several years of a merchant's payment technology budget, leaving no funds for acquiring the hardware necessary to accept payments that use other communications technologies. Moreover, activating hardware for other communication technologies would necessitate EMV recertification, adding to the adoption cost.

NFC technology is the favored technology of mobile wallets backed by EMV members (i.e., the Card Networks) because NFC payments "ride their rails." Indeed, MasterCard and Visa are among the Sponsor-level members of the NFC Forum, which controls the NFC technical specifications and provides NFC device manufacturers with compliance certification. *See supra* note 2. The EMV liability shift helps further the adoption of NFC, and this in turn benefits the Card Networks. Unless the Card Networks are taking steps to encourage device manufacturers to produce NFC-capable devices, however, this particular impact of the Honor All Wallets rules is unlikely to constitute an antitrust violation. *See infra* subsection II.B.3.f.ii.

f. *Possible Antitrust Violations*

i. Unreasonable Vertical Nonprice Restraint of Trade

Section One of the Sherman Antitrust Act prohibits every "contract, combination . . . or conspiracy in restraint of trade."[166] Since 1967, this language has been held to prohibit vertical nonprice restraints—contract terms imposed by a seller on a buyer that limit the terms on which the buyer may do business.[167] The Honor All Wallets rules are one such restraint because they limit the terms on which the ultimate buyer of a payment transaction (the merchant) may do business *on other transactions*, including the ability to take exclusively other types of payments over mobile devices.

A vertical nonprice restraint is not inherently illegal. Instead, the legality of vertical nonprice restraints, like almost all types of Section One violations, depends on whether it is an "unreasonable" restraint under antitrust's "Rule of Reason," which balances pro- and anti-competitive effects.[168] As typically applied, the Rule of Reason requires the plaintiff first to show that the restraint would have an adverse effect on competition in the relevant market, either by showing an actual likely adverse effect or by demonstrating that the defendant exercises market power (as a surrogate for actual effects). The burden then shifts to the defendant to show that there is a pro-competitive justification. If the defendant makes such a showing, the burden then shifts back to the plaintiff to show that the pro-competitive effects could be achieved via less restrictive means.[169]

Applying the Rule of Reason, it is clear that the Honor All Wallets rules likely have adverse effects on competition in the market for digital wallet services. The Honor All Wallets rules restrict merchants' ability to bargain about the terms under which they accept digital wallets and in so doing foreclose entry by digital wallets that utilize lower-cost payment systems like PIN-debit and ACH. Moreover, the Card Networks each likely have market power—the ability to materially affect prices—in the payment card market. As of 2016, Visa had a

166 15 U.S.C. § 1 (2012).

167 *See* Jeffrey M. Knetsch, Note, *A Uniform Rule of Reason for Vertical and Horizontal Nonprice Restraints*, 55 S. CAL. L. REV. 441, 441-442 (1982) (discussing United States v. Arnold, Schwinn & Co., 388 U.S. 365 (1967)). Although the classic vertical nonprice restraint is a geographical resale limitation, there is no prescribed form for a vertical nonprice restraint other than that it be a restraint on trade imposed on a buyer by a seller. *Id.* at 444-46.

168 *See generally* Phillip Areeda, The Rule of Reason in Antitrust Analysis: General Issues (June 1981), https://www.fjc.gov/sites/default/files/2012/Antitrust.pdf [https://perma.cc/CWA5-X6SR].

169 *See, e.g.*, Clorox Co. v. Sterling Winthrop, Inc., 117 F.3d 50, 56 (2d Cir. 1997). *But cf.* Gabriel A. Feldman, *The Misuse of the Less Restrictive Alternative Inquiry in Rule of Reason Analysis*, 58 AM. U. L. REV. 561, 583 (2009) (noting "there is no uniformity in the application or even statement of the [Rule of Reason] test, either across or within the federal circuits"). For an illustration of how the Rule of Reason applies to vertical nonprice restraints, see Bus. Elecs. Corp. v. Sharp Elecs. Corp., 485 U.S. 717, 720-25 (1988).

49% share of purchase volume on payment cards, MasterCard 21%, and American Express 11%.[170] All three Card Networks have been previously found to have market power in the credit card market,[171] and MasterCard and Visa have been found to have market power in the debit card market.[172]

Beyond the inevitable antitrust arguments over market definition and the presence of market power, the Card Networks' likely response to a challenge of their Honor All Wallets rules would be to argue that the rules are necessary to help them enter the digital wallet market given the presence of network effects. Put another way, the Honor All Wallets rules are necessary to break through the chicken-and-egg problem to ensure initial adoption of digital wallets.

The Card Networks would also likely raise a type of consumer benefit/consumer protection argument, based on the Second Circuit's holding that market definition (and market power analysis) in a two-sided network context requires analysis of effects on both sides of the market.[173] Thus the Card Networks would likely argue that if a merchant does not accept all digital wallets then cardholders will be liable to discover that, even though the store advertises that it accepts the Card Network's cards, his Card Network card on a digital wallet is not accepted. The consumer protection concern here is that the consumer would either suffer embarrassment at having payment denied or would ultimately be frustrated in his ability to perform a transaction, having reasonably relied upon the advertisement that the Card Network's cards were accepted and having brought only a digital wallet—not physical cards—to the store. Thus, the argument goes, the Honor All Wallets rules are necessary to protect the Card Network's payment system because if consumers are unpleasantly surprised, they might leave the system, thereby reducing the value of the system for all merchants because of network effects, and potentially setting off a vicious cycle of negative network externalities.

Finally, the Card Networks might make a policy argument encouraging the adoption of digital wallets by arguing that they represent a set of systemic improvements that benefit merchants and consumers and should be encouraged.

---

170 *See* NILSON REP., Oct. 2017, at 8, https://www.nilsonreport.com/publication_newsletter_archive_issue.php?issue=1119 [https://perma.cc/C9JT-TGFG].

171 *See* United States v. Am. Express Co., 88 F. Supp. 3d 143, 150 (E.D.N.Y. 2015), *rev'd on other grounds*, 838 F.3d 179 (2d Cir. 2016), *cert. granted*, No. 16-454, 2017 WL 2444673 (Oct. 16, 2017). For credit cards, Visa has a 46% market share, American Express 21%, and MasterCard 21% based on 2016 purchase volumes. NILSON REP., *supra* note 170, at 8; *see also* United States v. Visa U.S.A., Inc., 344 F.3d 229, 239 (2d Cir. 2003) (finding that MasterCard and Visa have market power in the credit and charge card network services market).

172 *See In re* Visa Check/Mastermoney Antitrust Litig., No. 96-CV-5238(JG), 2003 WL 1712568, at *3-4 (E.D.N.Y. Apr. 1, 2003). For debit cards, Visa has a 51% market share based on 2016 purchase volume, MasterCard a 22% market share, and the various PIN-debit networks combine for 18% market share. *See* NILSON REP., *supra* note 170, at 8.

173 *See Am. Express Co.*, 838 F.3d at 206.

In particular, digital wallets can offer improved transaction security and integrated advertising, coupons, rewards, and web browsing—a set of benefits which inure to both consumers and merchants. The Honor All Wallets rules, according to this argument, are necessary to facilitate the socially beneficial adoption of digital wallets (in part because of the network effects problem).

There is reason to be skeptical of these arguments. The network effects argument raises the question of whether a product is worthwhile if the only way it can successfully be adopted is through a vertical restraint of trade.[174] Moreover, many digital wallets are used for Internet-based payments, where the networks have long overcome any network effects problem; indeed, payment-card payments are the *dominant* form of Internet payments.

The consumer protection argument likewise does not ring true for digital wallets. Because there are no mandates requiring digital technology, a consumer with a digital wallet cannot reasonably be confident that any particular merchant will have the technical capability of accepting payments from a digital wallet. The reasonableness of consumer expectations is premised upon the existence of Honor All Wallets rules. Indeed, given the variety of form factors involved with digital wallets, it would not be reasonable for a consumer to expect universal acceptance, even if the digital wallet displayed a Card Network's logo. Consumers are all too familiar with the limitations of interoperability in the digital age; not everyone is able to accept every file format, for example—indeed, this is a reason for common file format standards, much like the common standards that exist for traditional plastic payment cards.

Moreover, to the extent that a digital wallet makes Internet payments, there is little risk of consumer embarrassment, as it would not likely be a point-of-sale transaction. Instead, the consumer would simply have to take another second to fish out a traditional plastic card for payment. Even for point-of-sale transactions, there is little harm from consumer embarrassment—being told that a digital wallet is not accepted is not the same as having a card declined—and most consumers still carry physical cards in physical wallets, not just digital wallets, and will continue to do so as long as various identity cards, such as drivers' licenses, employee ID cards, and transit passes are not digitized.

The systemic improvement argument is also lacking. Not only does it not have clear legal purchase, it is not even logical on its face. Digital wallets can *potentially* offer various improvements over plastic cards, but not all wallets actually do offer such improvements, and the Honor All Wallets rules do not discriminate among wallets. Indeed, the rules prevent such discrimination, meaning that the best wallets might not in fact win out. If the value proposition in digital wallets is

174 *Cf.* Polygram Holding, Inc. v. FTC, 416 F.3d 29, 38 (D.C. Cir. 2005) (noting that "if the only way a new product can profitably be introduced is to restrain the legitimate competition of older products, then one must seriously wonder whether consumers are genuinely benefitted by the new product").

sensible to merchants, then merchants will adopt them, especially given that merchants are already capable of accepting digital wallet payments that use communications technologies they already accept, such as magnetic stripe and NFC. If merchants were able to negotiate individual deals with digital wallet providers, they would likely adopt digital wallets *more* quickly, because there would be clear value propositions for acceptance of those wallets. The Honor All Wallets rules may thus actually *impede* the adoption of digital wallets.

Even if the various pro-competitive arguments are given credence, they are hardly the least restrictive alternative. First, any argument based on network effects would presumably hold only during the initial entry period; once network effects had been surmounted, then there would be no need for the Honor All Wallets rules. Thus, even if the Card Networks' arguments are accepted, the Honor All Wallets rules should be temporally limited. Second, there is no need to require acceptance of *all* devices in order to ensure the adoption of particular communications technologies, like NFC or QR codes. It is sufficient to require that merchants accept only specified devices. This would eliminate merchants' uncertainty over the risks posed by digital wallets.

All in all then, it would appear that there is a strong case that the Honor All Wallets rules would be found to be an illegal vertical nonprice restraint under the Rule of Reason.

ii. Unreasonable Restraint of Trade Through Tying

It is also possible to conceptualize the Honor All Wallets rules as tying arrangements. Not all tying arrangements are illegal; as the Supreme Court has noted, there are "[m]any tying arrangements . . . fully consistent with a free, competitive market."[175] Thus the sale of shoes together with laces or cars with tires is not thought to pose a competition problem, even though both products could be (and are) sold separately. It is only when tying functions to restrain trade that it violates the Sherman Act.[176]

Historically, the illegality of tying arrangements was evaluated using a "per se" standard that involved a four-part inquiry: whether (1) there are actually two distinct products or services; (2) there is an actual tying arrangement; (3) the defendant has market power for one of the products to which the other is tied; and (4) the tying affects a substantial amount of interstate commerce.[177] However, if the consumer would not have purchased the tied product absent the tying, there is no cognizable harm to competition, because competing

175 Ill. Tool Works, Inc. v. Indep. Ink, Inc., 547 U.S 28, 45 (2006).

176 *Id.* at 43-45.

177 Jefferson Par. Hosp. Dist. No. 2 v. Hyde, 466 U.S. 2, 9-16 (1984).

non-tied producers did not lose sales.[178] Instead, in such circumstances, the tying is nothing more than a price increase on the tying product.

Per se analysis, however, has largely fallen out of vogue in antitrust law; tying arrangements are one of the few areas in which it is still used, and even there its continuing vitality is in question. Instead, the per se standard has generally been replaced by the Rule of Reason, although the applicable standard depends in part on how the claim is framed. The per se rule has typically been applied to tying arrangements in which the defendant that has power in the tying product market will gain power in the tied product market. Indeed, in the Department of Justice's antitrust suit against Microsoft, the D.C. Circuit did not apply a per se analysis, but instead used a Rule of Reason analysis for platform software in "industries marked by rapid technological advance and frequent paradigm shifts."[179] Moreover, some tying arrangements are designed to help the defendant better maintain its market power in the tying product market. Such cases are likely to be reviewed under the Rule of Reason (as occurred in the Microsoft case).[180]

The Honor All Wallets rules have aspects of both situations. The Honor All Wallets rules function to tie the market for plastic card network services (the tying market) to the market for digital wallet network services (the tied market). The Card Networks' motivation for tying is to create market power in the digital wallet network services market. The resulting harm is foreclosure of entry to competing digital wallets that offer PIN-debit and ACH payments, meaning that both the competing digital wallets and their potential consumers (merchants and actual consumers) are harmed. This would seem to fit within the archetype for which the per se rule is designed.

On the other hand, there is certainly rapid technological advance in the payments industry, even if it is less than clear that digital wallets are a paradigm shift. Moreover, excluding PIN-debit and ACH digital wallets could be understood as a method of maintaining the Card Networks' existing market power in the overall payment card market as the market is transformed technologically. If so, then the focus would be on the tying product, rather than the tied product. Thus even if plastic Card Network services and digital wallet network services are not separate product markets (as opposed to distinct products), there could still be a tying problem. Viewed this way, however, a Rule of Reason analysis would be appropriate. The Rule of Reason analysis for a tying claim would look very similar to that for a vertical nonprice term restraint. The harm might be defined more broadly in a tying case focused on the tying product (namely the ability to swamp PIN-debit and ACH payment systems in general, and not just digital wallets using

178 *Id.*

179 United States v. Microsoft Corp., 253 F.3d 34, 79 (D.C. Cir. 2001).

180 *Id.*; *see also Ill. Tool Works*, 547 U.S. at 33-38.

those systems), but otherwise the analysis would seem to be the same, suggesting that tying claim might also be viable as an alternative approach.

If the per se test were ultimately applied, the Honor All Wallets rules would appear to be an illegal tying arrangement. The first element of the test requires two distinct products or services involved. The need to show two separate products is a proxy for efficiency; if the products are too closely related to each other (cars and engines; shoes and laces), then their bundling is assumed to be efficient and they are not viewed as separate products.[181] The tying in this case is formally between acceptance of traditional plastic cards and acceptance of digital wallets. The Card Networks, however, do not themselves offer plastic cards nor do they generally offer digital wallets. Instead, the Card Networks provide network services for both plastic cards and digital wallets.

Functionally, then, what the Honor All Wallets rules do is to tie together the market for network services for plastic cards with that for digital wallets. Digital network services include additional services beyond plastic network services, particularly related to tokenization. The test for distinct products under the per se rule is, at a minimum, whether there is consumer demand for both products separately.[182] The answer here is clearly yes, in that not all merchants accept digital wallets currently—for example, merchants who use only "knucklebusters" or take cards only by telephone orders—and therefore not all merchants demand digital wallet network services. Thus there are distinct services involved in the tying.

The second element requires an actual tying arrangement. This element is easily met. The Honor All Wallets rules are explicit contractual terms conditioning the acceptance of one payment device on the acceptance of another. As acceptance of these payments requires network services, it also means that if a merchant uses plastic network services, it is also required to use digital network services if presented with a digital wallet. Because each Card Network has a monopoly over network services for its own network, the Honor All Wallets rules also tie together plastic and digital network services. Although the Honor All Wallets rules are network rules, and the Card Networks do not contract directly with merchants, the Card Networks require acquirers to incorporate the Honor All Wallets rules in their contracts with merchants, giving merchants the privity needed to raise a tying claim based on the Honor All Wallets rules.[183] Thus the second element is readily met.

The third element is that the party imposing the tying arrangement must have sufficient economic power in the market for the base product to enable

---

181 *Cf. Jefferson Par. Hosp.*, 466 U.S. at 15-16.

182 *Id.* at 39 (Brennan, J., concurring) ("For products to be treated as distinct, the tied product must, at a minimum, be one that some consumers might wish to purchase separately *without also purchasing the tying product*.").

183 Moreover, merchants would have standing to bring an antitrust claim for this sort of injury because they are directly harmed by the reduction in competition.

it to restrain trade in the market for the tied product.[184] As noted above, all of the Card Networks likely have market power in the tying product market—the market for plastic card payments.

The fourth element, involving foreclosure of competition in a substantial amount of interstate commerce,[185] is also easily met—even though digital wallets are still a small percentage of retail payments, they are already a substantial dollar amount. The Honor All Wallets rules would therefore appear to be an illegal tying arrangement when analyzed under the per se rule, as well as under the Rule of Reason.

CONCLUSION

Different digital wallets present very different cost–benefit propositions to consumers and to merchants. For consumers, there is theoretically unrestrained ability to pick and choose whether to use a digital wallet or which wallet to use, which suggests that competitive pressure should address the risks digital wallets pose to consumers. Unfortunately, the types of risks digital wallets present are unlikely to be affected by competitive pressure because they are either not salient to consumers or because consumers cannot readily differentiate between wallets. This suggests the need for regulatory intervention by the CFPB to ensure minimum protections for consumers, particularly in terms of privacy, security, dispute resolution, and solvency.

For merchants, the variation in cost–benefit propositions among digital wallets is a much more vexing problem because merchants lack meaningful ability to pick and choose whether to accept digital wallets and on what terms. The Honor All Wallets rules force merchants to open a set of Pandora's Boxes. They also have the effect of raising barriers to entry for lower-cost digital wallets that make PIN-debit and ACH payments. Thus instead of technological advances *lowering* the cost of payments to merchants, the Honor All Wallets rules all but ensure that technological advances will *raise* the cost of payments to merchants and prevent them from engaging in beneficial partnerships with select digital wallet providers. Ironically, then, rather than facilitating the adoption of digital wallets, the Honor All Wallets rules are likely to impede the adoption of digital wallets overall. The Honor All Wallets rules should be the focus of serious antitrust and regulatory scrutiny.

Digital wallets hold out tremendous promise for reshaping retail commerce. Ensuring that they develop in a fair and competitive marketplace is key to realizing on that promise.

---

184 *Jefferson Par. Hosp.*, 466 U.S. at 13-14 (majority opinion).

185 *Id.* at 37 n.5 (Brennan, J., concurring).