PANDORA’S DIGITAL BOX:
DIGITAL WALLETS AND THE HONOR ALL DEVICES RULE

ADAM J. LEVITIN

MAY 31, 2016
PANDORA’S DIGITAL BOX:
DIGITAL WALLETS AND THE HONOR ALL DEVICES RULE

ADAM J. LEVITIN

EXECUTIVE SUMMARY

Digital wallets are software applications based on mobile devices, desktop computers, or the Web 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 then functions as a payment device for that account, transmitting the data to merchants to authorize payment. Data for multiple accounts can be stored in a single digital wallet, just as multiple payment cards can be stored in a physical wallet, allowing the consumer to select which account to use for payment.

Despite the functional similarities, payments from digital wallet present materially different risks and costs for merchants than traditional plastic card payments. Digital wallets can reallocate flows of consumer data from merchants to financial institutions and thus deprive merchants of valuable customer information used for anti-fraud, 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 tender choice and payment routing, increase fraud risk, subject merchants to patent infringement liability, and ultimately increase the costs of accepting payments.

The particular risks involved vary by digital wallet, but merchants are highly restrained in their ability to refuse or condition payments from digital wallets because of “Honor All Devices” rules promulgated by American Express, MasterCard, and Visa for merchants that accept payments with their network brands. The Honor All Devices rules require merchants to accept all network-branded payments from any device that uses a communications technology accepted by the merchant—magnetic stripe, Near Field Communications, Internet, etc. The Honor All Devices rules thus tie acceptance of a card network’s payments via digital wallets to the acceptance of traditional plastic cards that use the same communications technologies. The Honor all Devices rules force merchants to accept payments from all digital wallets utilizing a card network brand and thereby to open a digital Pandora’s Box that entails an unknown set of risks.

While the Honor All Devices rules impose various risks and costs on merchants, they also skew the competitive landscape for digital wallets. By preventing merchants from accepting only certain brands of payments from digital wallets, the Honor All Devices rules operate as interbrand restrictions on trade because they foreclose entry to digital wallets that make low-cost PIN-debit and ACH payments. The Honor All Devices rules thus artificially increase the market share of the high-cost credit and signature debt products of American Express, MasterCard, and Visa in the payment card network services market. The Honor All Devices rules should invite serious antitrust scrutiny because they produce cognizable harms to competition.
PANDORA’S DIGITAL BOX:
DIGITAL WALLETS AND THE HONOR ALL DEVICES RULE

ADAM J. LEVITIN*

INTRODUCTION ........................................................................................................................................... 2
I. DIGITAL WALLETS AND MOBILE PAYMENTS .................................................................................. 4
     A. Flows of Funds and Data in Traditional Credit and Debit Card Transactions ................................. 4
     B. Informational Value in Traditional Payment Card Transactions ..................................................... 5
     C. Digital Wallets .................................................................................................................................. 6
          1. Types of Digital Wallets .................................................................................................................. 6
          2. Mobile Wallets .................................................................................................................................. 7
     D. What Digital Wallets Change ............................................................................................................. 7
          1. Method of Transmission of Payment Authorization Data from Consumers to Merchants ............ 8
          2. Nature of Payment Authorization Data ........................................................................................... 9
               a. PCI-DSS Mandated Encryption .................................................................................................... 9
               b. EMV Chip Cards ............................................................................................................................ 11
               c. Tokenization ............................................................................................................................... 14
     E. Digital Wallets’ Impact on The Economics of Payment Card Networks .......................................... 16
II. THE HONOR ALL DEVICES RULES .................................................................................................... 18
     A. The Honor All Devices Rules ............................................................................................................. 18
     B. Problems Identifying Digital Wallets ................................................................................................. 20
III. RISKS INVOLVED WITH MOBILE WALLETS .................................................................................. 20
     A. Control Over Customer Data ............................................................................................................. 21
     B. Customer Relationship Management ................................................................................................. 23
     C. Tender Choice and Payment Routing .................................................................................................. 24
     D. Fraud and Data Security ..................................................................................................................... 26
     E. Intellectual Property Liability ............................................................................................................. 27
     F. Cost of Accepting Payments ............................................................................................................... 27
IV. ANTITRUST IMPLICATIONS OF THE HONOR ALL DEVICES RULES ............................................... 29
     A. From Honor All Cards to Honor All Devices ...................................................................................... 29
     B. Harms to Competition ......................................................................................................................... 30
     C. Possible Antitrust Violations ............................................................................................................... 33
          1. Unreasonable Vertical Non-Price Restraint of Trade ..................................................................... 33
          2. Unreasonable Restraint of Trade Through Tying ......................................................................... 36
CONCLUSION .............................................................................................................................................. 38

* Professor of Law, Georgetown University Law Center. Professor Levitin was commissioned to write this study by the Merchant Advisory Group, a retail industry trade association. The Merchant Advisory Group facilitated interviews with a number of its merchant members, but did not exercise any control over the content or conclusions of the study. The views presented in this study are Professor Levitin’s alone and do not necessarily represent the positions of the Merchant Advisory Group or its members.

© 2016, Adam J. Levitin
INTRODUCTION

Digital wallets are poised to transform the world of retail payments. 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 then functions as a payment device for the selected account, transmitting the data to merchants to authorize payment. By storing payment authorization data, digital wallets thus function analogously to physical wallets that contain multiple payment cards that can then be used to transmit payment authorization data.

Unlike traditional payment methods, such as checks and credit or debit cards, digital wallets can involve a range of form factors and communications technologies. All checks utilize a paper form factor, magnetic ink, and either manual data recordation or optical character recognition to transmit payment information. Credit and debit cards are standard-sized, plastic cards with magnetic stripes and embossed numbers. The magnetic stripes enable transmission of payment data by swiping the card through a card reader at point-of-sale, while the embossed numbers facilitate manual data transmission methods such as “knucklebusters”.

Digital wallets vary by form factor. While all digital wallets are software based, some are accessed through web-browsers, and others through mobile device apps. Web-based wallets store the consumer’s payment data in the cloud and can be accessed by any device with a web browser, be it a desktop or a mobile device. Other digital wallets are “mobile wallets” that run only on mobile devices, such as smartphones, tablets, wearables, or key fobs and dongles. Some wallets, such as Android 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 do not have a specific mobile app. Device-based mobile wallets can utilize a range of communications technologies for transmitting payment data from the device to merchants, including magnetic stripe emulation, Near Field Communication (NFC), Quick Recognition (QR) Code, Bluetooth, Bluetooth Low Energy, and instant messaging (SMS), as well as the Internet.

Digital wallets also vary by funding source and usability. Some digital wallets can fund payments from any credit or demand deposit account. Others are restricted to funding from a single bank or payment card brand or product. Likewise, some digital wallets can be used at a range of merchants, while others are for use at only a single merchant or consortium of merchants.

The different combinations of form factors, technologies, and business models involved in digital wallets pose different risks and costs for merchants, including the loss of valuable customer information, poaching of customers by competitors, impairment of customer relationship management, increased fraud risk, patent infringement liability, and increased costs of accepting payments.¹ Retailers, however, have only limited ability to refuse or condition acceptance of payments from digital wallets because of the “Honor All Devices” rules adopted by the three leading payment card networks, American Express, MasterCard and Visa (collectively, the “Card Networks”).

The Honor All Devices rules are one of the Card Networks’ several rules that restrain the terms on which merchants accept payments. The Honor All Devices rules require merchants that chose to

¹ Other risks, such as anti-money laundering law compliance, are beyond the scope of this study.
accept a Card Network’s payments using a particular type of communications technology to accept the Card Network’s payments without discrimination on all devices that utilize that communications technology.

For example, if a merchant accepts Visa contactless payments from credit cards with NFC chips, the merchant must also accept Visa contactless payments from all mobile devices that use NFC. The merchant could not accept only NFC payments from mobile devices that make payments through lower-cost payment systems like PIN debit and automated clearing houses (ACH). Likewise, under the Honor All Devices rules, 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 electro-magnetic field created by a magnetic stripe card.

A merchant, then, must accept payments from all form factors that utilize a technology if the merchant accepts any payments using the technology. As a result, merchants cannot refuse to accept payments from form factors that impose greater risks and costs upon them or to price for the risks created by that form factor. Indeed, merchants are unable to identify what form factor was used to make a payment.

The Honor All Devices rules mean that merchants lose control over what risks they accept and on what terms. Digital wallets can also shift control over payments and transaction data from merchants to the Card Networks and providers of digital wallets. Given the Card Networks’ past track record of using merchant restraint rules to maintain their market power, this shift of control is rightly worrisome to merchants. At the same time, digital wallets can diminish transactional informational flows to merchants, thereby frustrating fraud monitoring, customer service, advertising, and loyalty programs. In all, when accepting payment from a digital wallet, a merchant is forced to assume an unknown set of risks. Thus, digital wallets are a digital Pandora’s Box that the Honor All Devices rules force merchants to open if they want to take regular credit and debit payments—which is a sine qua non of participating in consumer retail markets.

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. Currently there is 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.

Even without technology mandates, however, there is no going backward in payment systems. Once a system is turned on, there’s no turning it off, as a business matter. Turning off a payment system risks alienating customers and losing transactions from customers who have relied upon acceptance of their system or device.

This study considers the potential issues digital wallets raise for retailers, including the antitrust implications of the Honor All Devices rules, which have the effect of foreclosing entry into the

---

2 NFC is a type of high-frequency radio frequency identification (RFID) communication. Both NFC and high frequency RFID operate under the ISO/IEC 14443 standard. The different terminology is because RFID usually refers to a combination of a separate “tag” and “reader” that communicate through an antenna, whereas an NFC card sometimes functions 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 the standards. The NFC Forum’s top-level members include MasterCard and Visa.

© 2016, Adam J. Levitin
digital wallet market for lower cost digital wallets and thereby help the Card Networks’ maintain their market power. The study begins with an examination of what digital wallets change in terms of the structure and economics of payment transactions. It then presents the Honor All Devices rules, before turning to a consideration of the risks and costs digital wallets can pose for merchants. A final section considers the Honor All Devices rules from an antitrust perspective.

I. DIGITAL WALLETS AND MOBILE PAYMENTS

A. Flows of Funds and Data in Traditional Credit and Debit Card Transactions

A traditional card-based payment, whether credit or debit, involves five parties: the consumer, the merchant, the consumer’s bank, and 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. 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 right on the transaction from the merchant. The acquirer acquires the transaction by paying the merchant an amount that is 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.

The payment card network promulgates the rules for the parties involved in the payment card network. 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 face. 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 schedules vary 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 valorem 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. Thus, merchants only have the ability to negotiate the acquirer’s merchant discount fee over and above the interchange fee.

---

3 See generally In re Payment Card Interchange Fee & Merch. Disc. Antitrust Litig., 986 F. Supp. 2d 207, 214 (2013). 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.

4 Acquirers will frequently outsource many of their functions to third-party independent service organizations (ISOs). Although ISOs play a major role on the ground 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.
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 the merchant. At each step of the way, however, the remitted funds are reduced by the associated offsetting fee: the interchange fee, the network fees, and the merchant discount fee. Figure 1 illustrates the flow of data and money in a payment card network.

**Figure 1. Payment Card Transaction**

![Figure 1](image)

### B. Informational Value in Traditional Payment Card Transactions

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 card transactions are much more informationally rich than cash transactions.

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 trip-wires for purchases made in unusual locations, at unusual times, for unusual amounts, or even for unusual items. For example, a customer with a history of purchasing geriatric products is unlikely to purchase a large quantity of energy drinks late at night. 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 purchased 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.

C. Digital Wallets

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

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 three dimensions: acceptance, funding, and form factor. Acceptance reference to where the wallet can be used to make payments. Some wallets “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, Android Pay, Samsung Pay, and PayPal all offer general purpose wallets, while retailers like Starbucks (which offers by far the most widely used mobile wallet), Walmart, Amazon.com offer single-business wallets, as do on-line retailers that store consumers’ payment information.

Second is how the wallet is funded. Some digital wallets are either “open wallets” that can be linked to any payment source (credit, debit, ACH with any payment network brand or bank) or “limited open wallets” that can be linked to a limited number of payment sources. 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 brand and bank specific. Yet other wallets are “closed wallets” that can be linked only to a single payment source from a single source. Thus far, all single business and multi-business wallets have been open wallets or limited open wallets. Table 1, below, summarizes the spending and funding possibilities for digital wallets.

---

5 Digital wallets may differ in an additional dimension, namely the unit of account they use for transactions. This study does not address digital wallets that utilize so-called crypto-currencies: private, digital currencies, such as Bitcoin, that are usually based on blockchain technology.
Table 1. Digital Wallet Funding and Spending Possibilities

<table>
<thead>
<tr>
<th>Open Wallet</th>
<th>Limited Open Wallet</th>
<th>Brand Wallet</th>
<th>Bank Wallet</th>
<th>Closed Wallet</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Purpose</td>
<td>• ApplePay</td>
<td>• Google Wallet (MC Debit)</td>
<td>• Chase Pay</td>
<td>• PAYTOO Wallet</td>
</tr>
<tr>
<td></td>
<td>• Android Pay</td>
<td></td>
<td>• Capital One Pay</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Coin</td>
<td></td>
<td>• Citi Wallet (MC only)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SamsungPay</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PayPal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Single Business Wallet</td>
<td>• Starbucks app</td>
<td>• Various online retail wallets</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Walmart Pay</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multi-Business Wallet</td>
<td>• Amazon.com</td>
<td>• CurrentC</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Square Wallet</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LevelUp</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Third, digital wallets vary by form factor. While all digital wallets are software based, some are accessed through web-browsers, and 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, be it a desktop or a mobile device. Some web-based digital wallets, such as PayPal and Google Wallet, are general purpose wallets, which are not specific to any particular merchant. Most web-based digital wallets, however, are business-wallets. 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, such as smartphones, tablets, wearables, or key fobs and dongles. Some, such as Android 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 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, Near Field Communication (NFC), Quick Recognition (QR) Code, Bluetooth, Bluetooth Low Energy, and instant messaging (SMS), as well as 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 might 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.

D. 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 design, although they may reallocate some of the value in the system and possibly increase costs, as discussed below in part III.F. To the extent that digital wallets also 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.6

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.

1. 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 business. 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 example, do not require a plastic card for access; they may also be accessed by checks or by the account and routing number for Automated Clearing House (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), or by manual input (such as with a “knucklebuster” or entry of the card information in a website), or, in recent years, through “contactless” transactions using Near Field Communication (NFC), that is radio-frequency ID chips embedded in the plastic card.

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, magnetic stripe emulation for transmission of payment data.7 The use of different data transmission technologies can potentially increase the risks faced by a merchant when accepting payments, as discussed below in part III.D and III.E.

---

6 In an ACH transaction, the merchant and consumers’ banks may charge additional fees, respectively, to the merchant and consumer.

7 The additional forms of data transmission are only feasible, of course, if a merchant is equipped to accept payments using such a technology.
2. 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 code (either the CVV1 that is encoded on a magnetic stripe or the CVV2 digits written on the back of the card) to the merchant.⁸ 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.

The payment 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 card network systems. The two primary security responses to the risk of theft of payment data are to reduce data retention by merchants and acquirers and to render payment data harder-to-use for thieves. Reducing data retention means that there is simply less payments authorization data sitting around for thieves to steal. Rendering data harder to use makes it less valuable and therefore less tempting.

a. PCI-DSS Mandated Encryption

The mechanism for forcing these security measures is the mandate of compliance with the Payment Card Industry Data Security Standard (PCI-DSS) promulgated by the Payment Card Industry Security Standards Council, an entity created and controlled by American Express,

---

⁸The precise terminology for the card verification code varies by card network. In this study, I refer to CVV1 (static, magnetic stripe data), CVV2 (static, back of card), and CVV3 (dynamic, EMV chip generated).
Discover, JCB International, MasterCard, and Visa.\textsuperscript{9} The Card Networks require that the acquirer banks ensure that their merchants comply with PCI-DSS (and hold the acquirers liable for assessments upon noncompliance),\textsuperscript{10} so acquirers require their merchants to attest that they are in compliance with PCI-DSS.\textsuperscript{11}

PCI-DSS version 3.1 restricts data retention, providing that “The 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.”\textsuperscript{12} 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.\textsuperscript{13}

PCI-DSS also requires that the 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, expiry date or service code) be rendered unreadable anywhere it is stored by encryption, hashing, or truncation methods.\textsuperscript{14} PCI-DSS also requires that sensitive information be encrypted for transmission over open, public networks, such as the Internet.\textsuperscript{15} Therefore, once a merchant receives cardholder data, the portion of that data that is deemed “sensitive authentication data” should never be stored post-authorization, while 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, such as the Internet.\textsuperscript{16} Transmission over in-house, private networks may still be done “in the clear.”

\begin{itemize}
\item \textsuperscript{10} See, e.g., Visa Rules § 1.10.4.1 (Oct. 16, 2015), at CR-77.
\item \textsuperscript{11} Historically the Card Networks have not required PCI-DSS compliance for smaller merchants. By early 2017, however, PCI-DSS will apply to small merchants as well. See Visa, Small Merchant Security Program Requirements—Update, at \url{https://usa.visa.com/dam/VCOM/download/merchants/bulletin-small-merchant-security-faq.pdf} (Jan. 31, 2017 compliance date).
\item \textsuperscript{12} PCI-DSS v.3.1, Requirement 3.1, p. 36 (April 2015), at \url{https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf}.
\item \textsuperscript{13} PCI-DSS v.3.1, Requirement 3.2, p. 37, p.8 (defining “sensitive authentication data”) (April 2015), at \url{https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf}.
\item \textsuperscript{14} PCI-DSS v.3.1, Requirement 3.4, p. 40 (April 2015), at \url{https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf}.
\item \textsuperscript{15} PCI-DSS v.3.1, Requirement 4.1, pp. 46-47 (April 2015), at \url{https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf}. PCI-DSS does not require encryption for transmission on internal networks, but it does not define what would constitute such a network, and data transmitted internally would also necessarily be stored, so there should be some level of encryption or truncation of the data under PCI-DSS Requirement 3.4.
\item \textsuperscript{16} 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 anti-fraud, advertising, loyalty, and customer service purposes.
\end{itemize}

© 2016, Adam J. Levitin
b. EMV Chip Cards

PCI-DSS relies on encryption as its primary security method. Encryption involves using a mathematical algorithm to scramble data, so that only someone who has decoding key can read the data. Another, distinct security technology is this use of integrated circuit cards (ICC), also known as “Chip” or EMV cards. Chip cards contain a microchip that is used with a special card reader to communicate with the microchip to verify that the card is a genuine card. The communications channel in a chip card payment is 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.

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. 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. The PAN and transaction-specific CVV3 is still transmitted “in the clear”—that is unencrypted—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. 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, but Chip technology does not prevent all counterfeit fraud. Creating a fully functional counterfeit Chip card 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 and co-existence of the magnetic stripe authorization channel, the lack of domain specificity for PAN

17 Encryption alone, however, does not equate to PCI compliance.

18 There is also an EMV contactless specification. It does not appear that any merchants in the United States are currently accepting 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 general low rate of contactless acceptance in the United States plus the certification costs of making contactless readers both EMV and PCI-DSS compliant.

19 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.

20 Alternatively, the transaction can be authorized in an off-line transaction by the merchant’s EMV terminal, which matches a public encryption key against the private encryption key on the card.

data, and the varying levels of card data verification used by issuers. The existence of multiple authorization channels that use data that is largely not specific to any particular channel enables fraudsters to arbitrage the differences in security measures for each channel.

For example, in a type of “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 milked data could then be encoded on a magnetic stripe card and used at a non-Chip terminal or at a Chip terminal utilizing the “fallback” function for non-functional Chip cards. While a diligent issuer should catch such arbitrages based on differences in the service code for Chip and magnetic stripe transactions, issuers’ verification procedures are not standardized.

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. Thus, one likely effect of the adoption of Chip technology will be the migration of fraud from card-present transactions to card-not-present transactions, as well as to card-present merchants that do not accept Chip transactions. Thus, a more accurate statement of the effect of Chip technology is that it makes it not cost-effective to make a fully functional Chip card, but it does not prevent all forms of card 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, LLC are American Express, JCB, Discover, MasterCard (which purchased Europay), UnionPay, and Visa. Significantly, the US PIN debit networks and ACH operators are not on the Board of Managers of EMVCo.

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, which are not co-owners of EMVCo) instituted a change in their rules that allocate liability for unauthorized card present transactions.


25 This was the experience with EMV adoption in the UK. See Mike Bond et al., Chip and Skim: cloning EMV cards with the pre-play attack, Computer Laboratory, University of Cambridge, at http://www.cl.cam.ac.uk/~rja14/Papers/unattack.pdf.

26 ATMs and automatic fuel dispensers are 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 being 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
Historically, for card-present transactions (which include contactless transactions\textsuperscript{27}), the card issuer was liable for unauthorized transactions provided that the merchant followed the requisite security procedures.\textsuperscript{28} 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 that 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 shift 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.\textsuperscript{29} The old liability rule for counterfeit card-present transactions remains in place if the card presented is not a Chip card, as well as for unauthorized transactions no involving counterfeit cards.\textsuperscript{30} 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 the liability rule shift outweigh the issuance cost, especially when reissuance is done as part of the normal card replacement cycle.

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.\textsuperscript{31} 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 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 subsequent PCI-DSS and EMV-compliance certifications relative to the merchant’s own anti-fraud benefits.

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

\textsuperscript{27}See, e.g., Visa Rules, Glossary (definitions for “Card-Present Environment” and “Card-Absent Environment” and “Face-to-Face”), at Glossary-742, Glossary 761.

\textsuperscript{28}Levitin, supra note 9, at 15. See also, e.g., Visa Rules, § 1.10.7, at CR-80-81.


\textsuperscript{30}Visa Rules, § 1.10.7, at CR-80-81; Visa Rules, § 4.1.22.57, at PSR-179; Visa Rules, § 5.9.2.6 at PSR-326.

\textsuperscript{31}See Visa, Transaction Acceptance Device Guide, Version 3.0, May 15, 2015, at 240, at http://technologypartner.visa.com/download.aspx?id=32; Visa, EMV Contactless Acceptance Requirements, Visa Business News, April 16, 2015. It is not clear how the cause of fraud (counterfeit, lost card, stolen card, fraudulent card application, account takeover) is 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.
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 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 anti-fraud, 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. This means that with Chip transactions, the merchant can correlate different transactions made with the same PAN, which facilitates anti-fraud, 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” that is the replacement of payment card data—the PAN and the card verification code—with randomly generated substitute data known as a “token”. The token will look like a PAN and card verification code, in that it will contain 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.”

Tokenization is not a necessary feature of digital wallets, but it appears to be an increasingly standard security. 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 a token to the merchant. The merchant will retain only the tokenized data, rather than the original encrypted PAN and card verification code. This tokenized data is useless to the hackers—but also to the merchant. Digital wallets potentially mask PANs by facilitating data “tokenization” before the data is even transmitted to the merchant.

---

32 See VISA CEO Confirms Tokens as New Network Revenue Stream, PYMNTS.com, Nov. 13, 2014 (quoting Charles Scharf, CEO of Visa).

33 This sort of acquirer tokenization does not eliminate data breach risk, but transfers it from the merchant to the acquirer, a sensible move only to the extent that acquirers maintain better security measures than merchants.
It is possible, however, to use a “multi-pay” token that is unique to both a PAN and a merchant. A multi-pay token is essentially a merchant-specific ersatz PAN. Such a multi-pay 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 on-line 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 e-Commerce merchants thus frequently use multi-pay tokenization. A multi-pay token also enables merchants to track a consumer’s transactions for anti-fraud purposes, and, if the merchant can correlate customer address or other identification information with the token, advertising, and loyalty program purposes.

Tokenization is also used by off-line 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 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.

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.

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 will retransmit it (through its acquirer) 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

---

34 Multi-pay tokenization can even be done with a Chip card as long as the initial Chip card verification was done offline.

35 A multi-pay token does, however, create the risk of on-us fraud following a data breach using the multi-pay token at the merchant.

36 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.
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, thereby frustrating anti-fraud measures, advertising and customer loyalty programs, and even potentially returns. Figure 3 shows how a token-generating digital wallet fits in a payment card network.

**Figure 3. Payment Card Transaction with Token-Generating Digital Wallet**

![Image of a payment card transaction with token-generating digital wallet]

**E. Digital Wallets’ Impact on The Economics of Payment Card Networks**

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 consumers. For example, on every ApplePay transaction, the card issuer pays Apple 15 basis points (0.15%) on the transaction volume. Those 15 basis points eat into the issuer’s bottom line. As the volume of ApplePay transactions increases, issuers will surely look to recoup those 15 basis points elsewhere. Similarly, the Card Networks themselves have indicated that they see digital wallets as a potential revenue source.¹⁷

To the extent that the 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

¹⁷ See VISA CEO Confirms Tokens as New Network Revenue Stream, PYMNTS.com, Nov. 13, 2014 (noting that Visa was waiving tokenization fees for 2015).
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.

Figure 4. Payment Card Transaction Economics

![Figure 4. Payment Card Transaction Economics](image)

Figure 5. Payment Card Transaction Economics with Digital Wallets

![Figure 5. Payment Card Transaction Economics with Digital Wallets](image)

38 Historically, in US PIN debit networks and in Australian EFTPOS transactions, fees flowed from issuers to acquirers.
II. THE HONOR ALL DEVICES RULES

A. The Honor All Devices 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 that are binding on their acquirer and issuer members. Card Network rules are incorporated by reference in merchant contracts. For example, Visa requires that acquirers have a merchant agreement with every merchant that takes Visa cards. Visa also requires that the merchant agreement to include language requiring the merchant to comply with the Visa Rules, including regarding Visa acceptance. Thus, even though merchants lack direct contractual dealings with Visa, they are nonetheless bound by its rules.

Among the Card Networks’ rules are “Honor All Cards” rules that require merchants to accept all cards carrying the Card Network’s logo. The Card Networks interpret their Honor All Cards rules to be “Honor All Devices” rules, meaning that merchants are required to accept all devices set up to transact through the Card Network, to the extent that the merchant accepts payments using the communications technology employed by the device. For example, Visa’s Honor All Cards rule states “A US 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.” A “Visa Card” is defined for the US region as “A Magnetic Stripe and/or a Visa Contactless Payment Device bearing the Visa Brand Mark, that enables a Visa Cardholder to obtain goods, services, or cash from a Visa Merchant or an Acquirer.” Thus at the 2013 fairness hearing for a proposed class action antitrust suit settlement, Visa’s attorney represented to the court that “the Master Card and Visa Honor-all-Cards Rules apply to both cards but also to other devices including contactless devices.”

Similarly, MasterCard requires “Merchants that choose to accept … MasterCard Cards to honor all … MasterCard Cards without discrimination when properly presented for payment.”

40 Visa Rules § 1.5.2.1 (Oct. 16, 2015) at CR-43. See also MasterCard Rules § 5.1.2 (“Each Merchant Agreement must contain the substance of each of the Standards set forth in Rules 5.4 through 5.11 [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.”).
41 Since a 2003 litigation settlement, there has been a carve-out 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.
42 It is unclear how the Honor All Devices 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 as 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.
43 Visa Rules § 1.5.4.5 (Oct. 16, 2015) at CR-53.
44 Visa Rules, Glossary-812.
45 In re Payment Card Interchange Fee and Merchant Discount Antitrust Litigation, MDL No. 1720, Transcript of Fairness Hearing, Sept. 12, 2013 at 38 (statement of Mr. Gallo).
MasterCard also expressly provides that unless otherwise stated, its rules regarding card acceptance also apply to non-card access devices.\footnote{MasterCard Rules, Dec. 11, 2014, pp. 255, 257 (definitions of “Access Device” and “Card”).}

American Express likewise requires that “Merchants must accept the Card as payment for goods and service ... sold, or (if applicable) for charitable contributions made at all Establishments, except as expressly permitted by applicable state statute.”\footnote{American Express Merchant Reference Guide – U.S., Oct. 2013, § 3.1, at 16.} American Express defines “Card” to mean “(i) Any card, account access device, or payment device or service bearing our or our Affiliates’ Marks and issued by an Issuer or (ii) a Card Number.”\footnote{American Express Merchant Reference Guide – U.S., Oct. 2013, at 58 (definition of “American Express Card or Cards”).} Thus, all three major payment card networks’ Honor All Cards rules are also Honor All Devices rules.

The Honor All Devices 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 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. 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 Android Pay.\footnote{Many US merchants that invested in accepting contactless NFC payments did so 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. The Honor All Devices rules plus the rise of NFC digital wallets may changes the implications of these merchants’ investment.}

The Honor All Devices rule not only requires acceptance of all wallets using a technology, but also non-discrimination among devices and among technologies. Therefore, a merchant that takes magnetic stripe payments must accept emulated magnetic stripe payments, such as those used by SamsungPay, \textit{without discrimination}. Similarly a merchant that takes NFC cards must accept all NFC devices, including devices running ApplePay and Android Pay wallets, \textit{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 Devices rule 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; instead, merchants are incentivized to partner with the Card Network itself to gain access to all wallets.

Currently, US merchants are not mandated to accept payments using any particular technology. This situation may well change, however. MasterCard has mandated that all card-present merchants in Europe accept contactless payments with NFC technology by 2020.\footnote{Press release, MasterCard, \textit{MasterCard Fast Tracks Mobile Payment Acceptance in Europe, Helping Europeans to Tap Everywhere by 2020}, Sept. 10, 2014, at \url{http://newsroom.mastercard.com/press-releases/mastercard-fast-tracks-mobile-payment-acceptance-europe-helping-europeans-tap-everywhere-2020/}.} In the United States, Visa has given indications that magnetic stripe technology is considered a legacy system that will be
phased out, as new cards and new contactless readers are required to support the quick Visa Smart Debit/Credit (qVSDC) interface in addition to the magnetic stripe data interface. US 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 Devices 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 smart phone, for example, using NFC communication, the merchant cannot determine whether an NFC-enabled card or a NFC-enabled digital wallet was used, much less which wallet on the smartphone was used. Likewise, some digital wallets, such as SamsungPay, use magnetic stripe emulation technology (“Magnetic Secure Transmission”) that mimics the electro-magnetic field created by a magnetic stripe transaction without ever swiping a card. A merchant cannot tell if SamsungPay has been used for a transaction or a traditional magnetic swipe card absent physical observation. While such observation is possible for some merchants, it is not possible for others, such as those with self-service kiosks or even at registers where the consumer is the party to handle the point-of-sale terminal.

The Card Networks have required card issuers to provide a “Form Factor Indicator” or “device type value” that can identify the device being used to make the transaction. Merchants interviewed for this study, however, 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, and even if they could they are prohibited from selective or conditional acceptance of digital wallets that use any particular communications technology through which the merchant accepts 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 involved in the particular wallets vary materially. In other words, the Honor All Devices rules tie acceptance of different types of payment devices using the same basic communications technology. Thus, 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.

**III. Risks Involved With Mobile Wallets**

There are several consequences of merchants not being able to identify or discriminate among digital wallets within any particular communications technology. Different wallets present different risks for merchants including terms of competition and control over customer data intellectual

---


53 See, e.g., Visa Rules § 4.1.22.10 (Oct. 16, 2015) at PSR-165; MasterCard Rules § 6.1.1, Dec. 11, 2014 (“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.”).
property liability, customer relationship management, control over tender choice and payment routing, fraud, data security, intellectual property liability, and cost of accepting payments.\textsuperscript{54}

\textbf{A. Control Over Customer Data}

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

The problem digital wallets present for merchants 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 not controlled by the merchant, nor even by that consumer. Instead, it is controlled by the digital wallet provider and/or the payment card network.\textsuperscript{55} Indeed, because of tokenization, digital wallets can result in an informational diminution for merchants (discussed in the following section). Thus, despite the greater informational wealth created by digital wallets, merchants come out worse in terms of value—not only does all of the additional value goes to other parties, 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 are the ones who can harvest and harness the additional data generated by digital wallet transactions. It is that there is nothing that prevents the 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.

For example, hypothetical fast food restaurant Tast-i-Fast could enter into a deal with a digital wallet provider under which Tast-i-Fast would get information on all of the digital wallet’s 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 of the merchant already exists with traditional plastic cards, but that information is of limited use with traditional plastic cards. 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 the consumer’s web searches. Nor would it be able to link the information to the consumer’s physical location. These factors limit the analytical value of the information. And even if Tast-i-Fast were able to come up with a compelling

\textsuperscript{54} Other risks, such as anti-money laundering law compliance, are beyond the scope of this study.

\textsuperscript{55} Aside from merchant issues, there is an additional level of competitive issues between the Card Networks and independent digital wallet providers. The Card Networks have at times exercised their market power to ensure that they are the entities that control the information generated by digital wallets. Thus, MasterCard imposed additional fees on “staged digital wallets,” like those of Google Wallet and PayPal, which do not pass along details of the transaction, such as a wallet ID and a merchant ID to MasterCard. These fees are meant to ensure that that data flows to MasterCard, so that it can construct a detailed profile of the cardholder’s spending habits. See Sarah Clark, \textit{MasterCard fights back against new payments players with increased transaction fees for digital wallets that don’t share data}, NFCWorld.com, Mar. 20, 2013, at http://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/.
insight from the information that it has, that would enable it to make a more attractive offer to consumers to steer purchases to it from Quick-i-Serve, it could not communicate that offer to the consumers in real time. At best, it could do targeted advertising and hope that the advertising’s message would not decay over time between the time of its receipt and the time of a purchase.

All of those 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 also real-time communication access to the consumer. Consider this scenario: Meg is a consumer with a smartphone-based digital wallet. In the prior months she has made a number of purchases of baby supplies and baby furniture with her digital wallet. Meg has gone to go shopping at The Store, a large retailer. As soon as she enters The Store’s parking lot, she receives a text message from her digital wallet provider. The text says “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 10% 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 on-line, 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 the general type of purchases she has been making; it is able to determine the stores she frequents (but not the exact items she purchases). It is also able to see her web searches, and because of a geo-location sensor in the smartphone, it is able to determine where Meg has gone and when. That allows the digital wallet provider to surmise the types of items Meg is likely to be interested in purchasing, and to identify when she is on the cusp of a potential purchase transaction. 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 for The Store, it’s not. The Store lost a sale of diapers. And The Store lost any potential impulse buys Meg might make. To the extent that Meg would have used a private-label or co-brand payment card at The Store, that revenue stream is also lost to The Store. The Store is getting scooped on its transactions because it has lost control over customer information because of the digital wallet.

Now consider the possibility that the digital wallet provider could itself be a large on-line retailer. The scenario above would allow such a retailer to scoop business away from brick-and-mortar retailers. The Honor All Devices rule prevents the brick-and-mortar retailer from taking steps to protect its business from this sort of poaching. If the brick-and-mortar retailer accepts Visa payments through Near Field Communication, 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.com were to offer a 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.com access to their customer information.

Payment companies already have insight into customer behavior in the case of co-branded cards (e.g., a United Airlines Visa), but a smart-phone digital wallet is a real-time communications channel with geo-location, enabling timely and targeted offers, advertisements, and coupons in a way that a co-branded card does not. Moreover, with a co-branded card, it is necessary to have the consumer sign up (and qualify for) for the card. Provision of a digital wallet is much simpler; the consumer has already signed up and qualified for the card(s) and just has to put them in the wallet.
Once that is done, the wallet provider or 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 a merchant transacts with a digital wallet, the merchant is surrendering data that could be used to poach future sales from the merchant. Every digital wallet transaction carries with it a set of competitive risks that does not obtain for traditional plastic cards. 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, the value a merchant receives with a digital wallet transaction is materially less than that with a traditional plastic card.

For some merchants the advent of device-based digital wallets presents an additional competitive threat. Some merchants already provide their own web-based digital wallets that can store payment card authorization data. These merchants have made a major investment to get consumer data and now face the prospect of disintermediation and loss of control over the data. Consider, for example, an airline. Airlines are primarily card-not-present merchants, but they do a small part of their business in card-present settings at ticket counters and on planes. Many airlines offer their own web-based digital wallets. The possibility that they will be required to accept other firms’ digital wallets for their card-present transactions raises the possibility that those competing digital wallets will also be used for card-not-present ticket purchases from the airline, thus diminishing the informational value to the airline of its own digital wallet.

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 sales associate at a merchant is unlikely to be able to assist because the sales associate will not be trained in the use of 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, loyalty programs, fraud prevention, and anti-money laundering law compliance. Tokenization interferes with these applications of the PAN. For example, if a husband and wife are both on a credit card account, they will both 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 its 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. 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 using an iPhone. Likewise, some token service providers, such as American Express, provide domain specific tokens, so a NFC payment would have a different token than a Chip transaction.\(^{56}\) 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.

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 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 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 either 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 (SARs).\textsuperscript{57}

EMVCo has developed a specification for a Payment Account Reference (PAR), a 29-digit alphanumeric sequence that would be consistent for an account regardless of form factor, but which could not itself be used to authorize payment. Use of PARs, however, is potentially expensive. First, merchants must adapt their systems to handle these 29-digit sequences. This can involve reprogramming thousands of point-of-sale terminals, which in turn, necessitate recertification of those terminals. Moreover, the PAR would be supplied by the token service provider—Visa, MasterCard, or Amex. The US 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 or 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 set-up 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 into 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 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

\textsuperscript{57} 31 U.S.C. § 5318(g)(1) (general requirement of SARs); 31 C.F.R. §§ 1020.320 (SARs for depositories), 1022.320 (SARs for money service businesses).
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 smart phones, like ApplePay and SamsungPay, offer consumers the possibility of authorizing 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 US 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.

For tokenized devices, the requirement of EMVCo certified tokens for EMV-compliant wallets that qualify for the EMV liability shift also has an indirect effect of shifting tender. The only EMVCo certified token providers are reportedly EMVCo’s owners—Visa, MasterCard, and American Express. There is no certification specification, and thus no path to certification, for competing networks, such as PIN debit networks. EMVCo’s limited certification of token providers heavily favors Visa, MasterCard, and American Express because issuers that want to get their cards onto tokenized digital wallets and benefit from the EMV liability shift must work with them.

Visa, MasterCard, and American Express’s role as token providers also gives them a line of sight to the authorization and response on all tokenized transactions on mobile wallets, not just those routed through their networks, because of the role of the token provider in detokenizing the transaction. Visa, MasterCard, and American Express can see all of the tokenized transactions on PIN debit networks for which they provide the token. This information gives Visa, MasterCard, and American Express a significant advantage over PIN debit networks when negotiating with issuers and acquirers. It also creates the possibility of the Card Networks selling the information and associated analytics.

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.

There is differential ease of use for different types of payments. 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.

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, and that merchants be allowed determine the routing of the transaction. For magnetic stripe transactions, merchants are able to

---

choose the routing based on the bank identification number (BIN) on the card. For domestic Chip transactions, the routing selection is done through software on the merchant’s point-of-sale Chip terminal called the Common Application Identifier (Common AID) that selects between different routing applications on the Chip card’s chip.

The use of a mobile wallet potentially enables the cardholder to override use of the Common AID in favor of a separate Global AID (which does not contain 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 (e.g., a choice between “Visa debit” and a generic “US debit”). 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 in the interim leave the merchant exposed to counterfeit fraud liability under the EMV liability shift rule. 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 at 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 on fake or unauthorized accounts onto digital wallets. This was a significant problem with ApplePay’s initial rollout. 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 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 Devices rules and lack of ability 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 wallet, such as ApplePay, that would allow ApplePay 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 Devices rules, however, 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 against 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 study 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 payments communication medium, they have little ability to protect themselves against potential patent infringement liability other than by negotiating with their acquirer banks for indemnification. The acquirer banks, however, themselves 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.”\[^{61}\] 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 is an additional mouth 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 15 basis points on every ApplePay transaction. These 15 basis points are paid by the card issuer, which reduces the issuer’s profits. As ApplePay’s transaction volume grows, these 15 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 7¢ per token and 2¢ per decline, which it waived for the first year, before later suspending the fee for issuers that do their processing through Visa. It would not be surprising if Visa were to reinstitute the fees once issuers have committed sufficiently to tokenization of transactions, so as to be locked into using tokenized transactions.

Similarly, MasterCard has created “digital enablement fees” for both issuers and acquirers. Issuers are subject to 50 cent “digitization” fee for the provision of a token and a “Digital Enablement Service Lifetime Management” fee of 10 cents per month for tokenized PAN, as well as a fee of 2.5 cents for calls to its “alternative network application programing interface”. Acquirers are charged 1 basis point on select card-not-present transaction volumes.

It is unclear whether the market for tokenization services will be competitively priced once it is fully established. The Card Networks are reportedly the only entities licensed by EMVCco (which they own) to serve as token service providers under EMV specifications. It is currently unclear if the Card Networks compete for token service provision business. That is, can American Express serve as a token service provider for a Visa card? Presumably the answer is no for all functional purposes, even if there is no formal prohibition.

Additionally, as discussed above, the networks are likely to charge for Payment Account Reference numbers that stand in for a Payment Account Number 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 to 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 business sense for a merchant to accept a digital wallet. Because of the Honor All Devices rules, however, merchants are not able to select which digital wallets they wish to accept and on what

---


63 The 2006 and 2008 spin-offs of MasterCard and Visa, respectively, by the issuers that had previously owned them likewise put pressure of network fees because of the need to generate revenue for public shareholders.

64 VISA CEO Confirms Tokens as New Network Revenue Stream, PYMNTS.com, Nov. 13, 2014 (noting that Visa was waiving tokenization fees for 2015).

terms. The result is to preclude merchants from protecting their own interest or from seeking out favorable deals with individual digital wallet providers.

IV. ANTITRUST IMPLICATIONS OF THE HONOR ALL DEVICES RULES

The Honor All Devices rules raise credible antitrust concerns about illegal restraint of trade.\(^66\) The Honor All Devices 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 Devices rules’ restraint on merchants, there would more likely be entry by competing digital wallets offering cheaper payments using PIN debit and automated clearing houses (ACH).

The Honor All Devices 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 Devices rules should invite serious scrutiny by competition regulators and could presage private litigation.

A. From Honor All Cards to Honor All Devices

The Honor All Devices rules are an expanded interpretation of the Card Networks’ Honor All Cards rules.\(^67\) 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.\(^68\) The variation among issuers is immaterial to merchants; all issuers (and acquirers) are FDIC-insured financial institutions, and the payments from the issuers to the acquirer are guarantied by the Card Network.\(^69\) 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 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. 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.

\(^66\) 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 joint venture and of its reported limited licensing of its tokenization specification is beyond the scope of this study.

\(^67\) The Honor All Cards rules are part of a battery of Card Network rules that restrain merchants’ ability to bargain for the terms on which they accept particular payment cards. These other rules (sometimes called “merchant restraints”) include restrictions surcharging for more expensive transactions, limitations on minimum and maximum transaction amounts, prohibitions on the processing of a Card Network’s transactions over other networks, and requirements that merchants that accept cards to take them at all of their locations. Adam J. Levitin, \textit{Priceless? The Economic Costs of Credit Card Merchant Restraints}, 55 UCLA L. REV. 1321, 1334-38 (2008).

\(^68\) See \textit{In re Visa Check/MasterMoney Antitrust Litig.}, 192 F.R.D. 68, 73 (E.D.N.Y. 2000).

The Honor All Cards rule also historically tied acceptance of the Card Networks’ credit cards to the acceptance of the Card Networks’ signature debit cards. Signature debit cards—cards for which transactions are authorized by a signature rather than by entry of a PIN—have higher interchange fees than PIN debit cards and are inherently less secure, increasing chargeback risk for merchants. 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 and thus enabled entry into the payments market by an inferior product at the expense of the PIN debit networks’ 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. The second round of litigation focused on the tying of rewards cards with non-rewards cards (a tying bolstered by certain other Card Network rules) and resulted in a not-yet-finalized $7.25 billion class action settlement (with numerous class action opt-out suits still being litigated).

The Honor All Devices rules are formally interpretations of the Honor All Cards rules. Functionally, however, they are new restraints that enable the Card Networks to maintain their market power in the credit and debit card markets, both in terms of card acceptance for merchants and 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 Devices 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 Devices rules do more than the Honor All Cards rule. The Honor All Cards rules were an intrabrand restriction: Honor All Cards rules required a merchant that accepted one Visa card to accept them all. The Honor All Devices rules function as an interbrand 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 (or PIN debit or ACH) NFC payments on from mobile wallets. Because a digital wallet can contain multiple brands’ cards, the Honor All Devices rules functions as an interbrand restriction, not merely an intrabrand restriction. This difference is significant, because antitrust law is much more skeptical of interbrand restrictions than intrabrand restrictions.

B. Harms to Competition

Antitrust law is about protecting competition, not competitors. Therefore, antitrust violations require injuries to competition. Although the Honor All Devices rules restrict merchants’ ability to bargain for the terms under which they accept payments and has the effect of imposing significant risks and costs of merchants, that alone is not an injury to competition and therefore the grounds

---

70 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.


for antitrust liability. Instead, the Honor All Devices rules injure competition by restricting competition for network services at point-of-sale (as opposed to on-line). This has the effect of foreclosing the entry of digital wallets that utilize lower-cost point-of-sale payment methods, such as PIN debit and ACH payments. Not only does this foreclosure harm competing digital 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 Devices rules, it is not clear that there would be a market for open wallet 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. All consumers with digital wallets 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 consumption and therefore more sales to merchants. 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.

Digital wallets, however, need not make Card Network payments. Instead, they can make payments using ACH or PIN debit cards, such as with the PayPal and CurrentC digital wallets. 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 Devices rule, 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 Devices rule gets the Card Networks around the problem that merchants are not generally attracted to digital wallets that use their cards. The Honor All Devices rule prevents merchants from being able to accept digital wallets selectively or conditionally if the merchant also takes plastic cards. A merchant might well want to accept only ACH and PIN debit payments from

---

73 Even aggregators such as PayPal strive to steer customers away from funding their wallets with the Card Networks’ cards because of their high cost. Adam J. Levitin, Payment Wars: The Merchant-Bank Struggle for Control of Payment Systems, 12 STAN. J. L. BUS. & FIN. 425, 480-81 (2007).

74 ACH payments can be either push or pull payments.
digital wallets, but cannot under the Honor All Devices rule. Instead, the merchant must also accept
digital wallets that make payments on the Card Network’s credit and signature debit networks.

Absent the Honor All Devices rule, merchants might simply refuse to accept credit and
signature-debit-based digital wallets. 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
Devices rule thus helps the Card Networks gain entry to the digital wallet market despite offering
non-competitive products.

The Honor All Devices rule does more than help the Card Networks gain entry into the digital
wallet market, however. 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). 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. 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 type of participants in
the system. The more merchants accept a payment method, the more valuable the payment method
is to consumers and vice versa.

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.75 Whereas consumers are likely
to use multiple on-line 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 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 Devices rules help the Card Networks 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 to incentivize them to use the digital wallets with the Card

75 Mobile wallets involve a second layer of network effects relating to the specific device. Consumers are likely to
select mobile devices based on attributes other than digital wallets, so a consumer’s digital wallet choices are
circumscribed by the initial choice of device.

© 2016, Adam J. Levitin
At present, the NFC technology is the favored technology of mobile wallets backed by EMV members 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. NFC Forum, Our Members, at http://nfc-forum.org/about-us/our-members/. The EMV liability shift helps further the adoption of NFC, despite its security risks as compared to other communication technologies, such as QR codes, and this in turn benefits the Card Networks. Unless the Card Networks are taking steps to encourage device manufacturers to produce NFC-capable devices, this particular impact of the Honor All Devices rules is unlikely to constitute an antitrust violation.

© 2016, Adam J. Levitin
A vertical non-price restraint is not inherently illegal. Instead, the legality of vertical non-price restraints, like almost all types of section 1 violations, depends on whether it is an “unreasonable” restraint, with the reasonableness evaluated under a test known as the “Rule of Reason” that balances pro- and anti-competitive effects. 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.

Applying the Rule of Reason, it is clear that the Honor All Devices rules likely have adverse effects on competition in the market for digital wallets. The Honor All Devices rules restrict merchants’ ability to bargain about the terms under which they accept digital wallets and in so doing forecloses entry to 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 2014, Visa had a 46% share of purchase volume on payment cards, MasterCard 21%, and American Express almost 13%. All three Card Networks have been previously found to have market power in the credit card market, and MasterCard and Visa have been found to have market power in the debit card market.

The Card Networks’ likely response to a challenge of their Honor All Devices rules would be to argue that the rule is necessary to help them enter the digital wallet market given the presence of network effects. The Honor All Devices rule is 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 protection argument, namely that if a merchant does not accept all digital wallets then cardholders will be liable to discover when at the cashier that his Card Network card on a digital wallet is not accepted, even though the store advertises that it accepts the Card Network’s cards. 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 Devices rules are necessary for protecting 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.

80 See NILSON REPORT, #1074 at 8 (Oct. 2015).
81 United States v. Visa U.S.A., Inc., 344 F.3d 229, 239 (2d Cir. N.Y. 2003) (finding that MasterCard and Visa have market power in the credit and charge card network services market); United States v. Am. Express Co., 88 F. Supp. 3d 143, 187-207 (E.D.N.Y. 2015) (finding American Express to have market power in the general purpose credit card market in the United States). The American Express ruling is currently on appeal. For credit cards, Visa has a 47% market share, American Express 25%, and MasterCard 23% based on 2015 purchase volumes. NILSON REPORT #1080 at 8 (Feb. 2016).
82 In re Visa Check/Mastermoney Antitrust Litig., 2003 U.S. Dist. LEXIS 4965, *23-24 (E.D.N.Y. Apr. 1, 2003) (finding Visa alone and Visa and MasterCard combined have market power in the debit card services market). For debit cards, Visa has a 51% market share based on 2014 purchase volume, MasterCard a 21% market share, and the various PIN debit networks combine for 19% market share. See NILSON REPORT, #1074 at 8 (Oct. 2015).
Finally, the Card Networks might make a policy argument about encouraging the adoption of digital wallets because they represent a set of systemic improvements that benefits merchants and consumers in general that should be encouraged. In particular, digital wallets can offer improved transaction security and integrated advertising, coupons, rewards, and Web-browsing, a set of benefits that can inure to both consumers and merchants. The Honor All Devices rule, according to this argument, is 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 all 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 on trade. 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 does not ring true for digital wallets. Because there are no technology mandates, a consumer with a digital wallet cannot reasonably be confident that any particular merchant will have the technical capability of accepting payments from the wallet. The reasonableness of consumer expectations is premised upon the existence of an Honor All Devices rule. 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 the consumer embarrassment—being told that a digital wallet is not accepted is not the same as having a card declined for being overlimit, for example—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 and 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, but it is not even obviously correct on its face. Digital wallets can potentially offer various improvements over plastic cards. But it is not true about all wallets, and the Honor All Devices 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 sensible to merchants, then merchants will adopt them, especially given that merchants are already capable of accepting digital wallet payments that use communications technologies merchants already accept, such as magnetic stripe and NFC. Indeed, 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 Devices 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 Devices rules. Thus, even if the Card Networks’ arguments are accepted, the Honor All Devices 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 Devices rule would be found to be an illegal vertical non-price restraint under the Rule of Reason.

2. Unreasonable Restraint of Trade Through Tying

It is also possible to conceptualize the Honor All Devices rules as tying arrangements. Not all tying arrangements are illegal, as the Supreme Court has noted, there are “[m]any tying arrangements … [that] are fully consistent with a free, competitive market.” 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 is a Sherman Act section 1 violation.

Historically, the illegality of tying arrangements was evaluated using a “per se” standard that involved four-part inquiry, namely whether (1) there are actually two distinct products or services, (2) there is an actual tying arrangement, (3) defendant has market power for one of the tied products (the “tying product”) to which the other is tied (the “tied product”), and (4) the tying affects a substantial amount of interstate commerce. If the consumer would not have purchased the tied product, absent the tying, however, there is no cognizable harm to competition, as competing non-tied producers did not lose sales. 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, but its continuing vitality is in question. Instead, the per se standard has generally been replaced by the Rule of Reason.

Which rule would ultimately apply to a tying claim depends, in part on how the claim is framed. The per se rule has typically been applied to situations in which the claim is that the defendant that has power in the tying product market will gain power in the tied product market, and the four-part per se test is geared to such harms. Indeed, in the Department of Justice’s antitrust suit against Microsoft, the Court of Appeals for the District of Columbia Circuit did not apply a per se analysis, but instead used a Rule of Reason analysis for platform software in “industries market by rapid technological advance and frequent paradigm shifts.”

Moreover, some tying arrangements are designed to allow the defendant to 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).

The Honor All Devices rules have aspects of both situations. The Honor All Devices 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.

86 United States v. Microsoft, 253 F.3d 34, 65, 84 (D.C. Cir. 2001).
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 about 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 non-price 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 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 Devices 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 so 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. The tying in this case is formally between acceptance of traditional plastic cards with 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 Devices rules do is to tie together the markets for network services for plastic cards (“plastic network services”) with that for digital wallets (“digital network services”). 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. 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 Devices rules are explicit contractual term 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 Devices rules also tie together plastic and digital network services. Although the Honor All Devices rules are network rules, and the Card Networks do not contract directly with merchants, the Card Networks require acquirers to incorporate the Honor All Devices rules in their contracts with merchants, giving merchants the

---

87 MasterCard is a partner in the Google Wallet product, but allows its cards to be used on other digital wallets.
88 Merchants access these network services markets only indirectly, through their acquirers.
privity needed to raise a tying claim based on the Honor All Devices rules. 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 it to restrain trade in the market for the tied product. 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 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 Devices 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

The Honor All Devices rules are the third incarnation of the antitrust problems that have arisen under the Honor All Cards rules. The problems created by the Honor All Devices rules, however, are more complicated for merchants than those posed by the traditional Honor All Cards rules. The Honor All Cards rules tied credit and signature debit cards together as well as rewards and non-rewards cards. The differences for merchants between signature and PIN debit and rewards and non-rewards cards were primarily differences of pricing; merchants were being compelled to accept more expensive cards in order to accept cheaper ones, and the more expensive cards do not produce any additional benefit for merchants. The price differences were, however, often visible to merchants in advance, at least giving merchants the theoretical option of pricing whether it was worthwhile accepting the bundled products.

The Honor All Devices rules are different, in that the risks that merchants are compelled to accept under the rule are not always easily quantifiable price terms. The Honor All Devices rules compel merchants to accept digital wallets that are Pandora’s Boxes, of varied and unknown risks. A merchant cannot know if by accepting NFC payments, for example, it will be opening a window into its transactions for a competitor, or whether it will be exposing itself to a patent infringement suit. These risks are real, but the probability and magnitude of these risks are difficult to estimate. The Honor All Devices rules thus impose a set of serious, but hard to quantify risks on merchants. While these harms are real, they are not a cognizable antitrust injury. Instead, the antitrust problem presented by the Honor All Devices rules is that they also operate to raise barriers to entry to 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 Devices rules all but ensure that technological advances will raise the cost of payments to merchants. The result is likely to impede the speed of adoption of digital wallets overall.

The fact that this is the third round of antitrust problems with the Card Networks’ merchant restraint rules is also a strong indication of the inadequacy of the settlements in the prior rounds of litigation. The prior rounds’ settlements addressed specific applications of the merchant restraint rules, but left the door open for other applications. As long as the Card Networks continue to exercise market power, their merchant restraint rules are likely to remain problematic. Given the

90 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.
glacial speed of antitrust litigation and the rapid pace of technological change, addressing these problems through the courts is likely to be a slow-motion game of antitrust Whack-a-Mole. Litigation may simply not be a sufficient tool for solving the problem long-term; instead, the persistent problems stemming from the concentrated market power of the Card Networks may require regulatory interventions.