UNC SCHOOL OF LAW

NORTH CAROLINA BANKING INSTITUTE

Volume 20 | Issue 1 Article 16

3-1-2016

Less is NOT More: The Need to Regulate Apple Pay

Maxwell L. Gregson

Less is NOT More: The Need to Regulate Apple Pay

I. INTRODUCTION

Twenty-five percent of American adults own an iPhone.[1] All model 6 and newer iPhones are Apple Pay-enabled and in a matter of a few years, all the non-Apple Pay-enabled iPhones will likely be replaced.[2] Now, combine Apple's broad reach with the recent development that social security and veteran beneficiaries may upload their federal benefit debit cards to Apple Pay.[3] This is possible because Apple Pay is permitted as a platform for federal payment cards that are used to disburse social security and veterans' benefits.[4] In addition, Apple Pay now supports financial transactions with the federal government, on the receiving end, such as admission to national parks.[5] This means that the federal government is now both a card issuing institution and a merchant that has a formal agreement with Apple Pay.[6] By adopting Apple Pay as a mobile payment platform, the government is subjecting itself, and the taxpayers, to the risk that criminals will exploit the vulnerability of the Apple Pay system, just as it does with the current debit card system.[7] The difference is that, under the current regulatory

---

1. Philip Elmer-DeWitt, *NPD: Better Than 1 in 4 Adult Americans Now Own an iPhone*, TIME INC. NETWORK: FORTUNE (Jan. 16, 2014, 8:33 PM), http://fortune.com/2014/01/16/npd-better-than-1-in-4-adult-americans-now-own-an-iphone/.

2. *See* Farhad Manjoo, *A Wild Idea; Making Our Smartphones Last Longer*, N.Y. TIMES (Mar. 12, 2014), http://www.nytimes.com/2014/03/13/technology/personaltech/the-radical-concept-of-longevity-in-a-smartphone.html?_r=0 (detailing how the average user only keeps an internet-enabled mobile phone for two years before purchasing a newer model and therefore most people will have all the technological advancements that come along with those newer models).

3. Tim Higgins & Elizabeth Dexheimer, *Obama's Visit to Silicon Valley is a Big Win for Apple Pay*, BLOOMBERG BUS. (Feb. 13, 2015, 2:36 PM), http://www.bloomberg.com/news/articles/2015-02-13/obama-s-visit-to-silicon-valley-is-a-big-win-for-apple-pay (explaining how the federal government has publicly endorsed the payment platform, Apple Pay, for use in limited federal transactions).

4. *Id.*

5. *Id.*

6. *See id.* (explaining Apple Pay and how the federal government is now allowing their customers to utilize Apple Pay).

7. Sophia Yan, *Thieves Use Stolen Credit Cards on Apple Pay – Report*, CNN MONEY (Mar. 5, 2015, 10:11 PM), http://money.cnn.com/2015/03/05/technology/apple-pay-

regime, the government would be the party responsible for this fraud, not Apple Pay.[8] Because technology failure is a leading cause of distrust of both the federal government and private companies, the security of Apple Pay will, and should be in the public's and the government's forethought.[9]

Apple Pay is a different animal than other forms of mobile payment, particularly in regards to its current lack of regulation.[10] This lack of regulation, combined with the evolving technology, presents a unique security threat.[11] The burden on Apple of implementing additional security measures for Apple Pay, as might be required by further federal regulation, does not outweigh the benefits the platform provides to banks, merchants, the government, and consumers.[12]

This Note proceeds in five parts. Part II of this Note illustrates the current landscape of the mobile payment industry and provides a comparison of the functional characteristics and security measures of the industry's major players.[13] Part III examines how Apple Pay differs from its competitors, both with regard to its business model and current security technology.[14] Lastly, in Parts IV and V, this Note explores Apple

---

hack/index.html?iid=EL (explaining how a thief can load a stolen credit or debit card onto Apple Pay and use that stolen card to pay for items).

8. *See* Andrew Ross Sorkin, *Pointing Fingers in Apple Pay Fraud*, N.Y. TIMES (Mar. 16, 2015), http://www.nytimes.com/2015/03/17/business/banks-find-fraud-abounds-in-apple-pay.html?_r=0 (explaining how banks are financially responsible when fraud occurs via Apple Pay, therefore the federal government would be responsible in the same manner).

9. *See* Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RESEARCH CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ (explaining how only 25% of people surveyed are even somewhat confident that the government will keep their information secure and that number is only marginally better at 29% for credit card companies).

10. *See* Samuel Rubenfeld, *Apple Pay Faces Lighter Compliance than Paypal, Google*, WALL ST. J.: RISK & COMPLIANCE J. (Oct. 20, 2014, 5:45 AM), http://blogs.wsj.com/riskandcompliance/2014/10/20/why-apple-pay-faces-lighter-compliance-than-paypal-google/ (explaining how Apple Pay has not registered with the Financial Crimes Enforcement Network ("FINCEN") like its competitors).

11. *See id.*

12. *See* Shane Cole, *How Apple Pay is Designed to Avoid the Pitfalls of Traditional Payment Systems*, APPLEINSIDER (Oct. 20, 2014, 5:26 AM), http://appleinsider.com/articles/14/10/20/how-apple-designed-apple-pay-to-avoid-the-pitfalls-of-traditional-payment-systems (explaining how security threats are a constant worry regarding payment technology and how Apple Pay is a different payment platform gaining support due to its purported ability to protect consumer privacy).

13. *See infra* Part II.

14. *See infra* Part III.

Pay's current regulations and Apple Pay's future should it become subject to the current regulation regimes for the payments industry.[15]

II. WHAT ARE MOBILE PAYMENT SERVICES AND WHY ARE THEY BECOMING POPULAR?

Electronic and mobile payment services have been a part of mainstream culture since 2002, which is when eBay bought PayPal and utilized it for more than just eBay transactions.[16] Mobile payment methods primarily serve to replace physical currency by utilizing an internet-enabled mobile phone or tablet.[17] Although there are many mobile payment services available to users, and new services are released seemingly every day, an overview of some of the main services in today's market is helpful to understand the current state of the industry.

A. PayPal

PayPal, founded in 1998,[18] can be viewed as the baseline for electronic payment services.[19] It is geared more toward internet purchases and less toward payments made with a user's mobile phone, although PayPal does have a mobile application ("App") for internet-enabled mobile phones and other portable devices.[20] PayPal facilitated $66 billion in mobile payments in 2015,[21] out of total payment volume of $282 billion,[22] among their 179 million users.[23] A PayPal user links a

15. *See infra* Parts IV, V.

16. Margaret Kane, *eBay Picks Up PayPal for $1.5 Billion*, CNET (Aug. 18, 2002, 1:50 AM), http://www.cnet.com/news/ebay-picks-up-paypal-for-1-5-billion/.

17. Robert C. Drozdowski et al., *Mobile Payments: An Evolving Landscape*, FED. DEPOSIT INS. CORP.: SUPERVISORY INSIGHTS - Winter 2012, https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin12/mobile.html#twelve (last updated Jan. 03, 2013).

18. *Who We Are*, PAYPAL ABOUT [hereinafter PAYPAL ABOUT], https://www.paypal.com/webapps/mpp/about (last visited Nov. 17, 2015).

19. *See id.* (explaining how PayPal is constantly at the forefront of the ever-changing mobile payments market).

20. *See id.*

21. PAYPAL ABOUT, *supra* note 18.

22. *Id.*

23. *Number of PayPal's Total Active Registered User Accounts From 1st Quarter 2010 To 4th Quarter 2015 (In Millions)*, STATISTA, http://www.statista.com/statistics/218493/paypals-total-active-registered-accounts-from-2010/ (last visited Feb. 7, 2016).

debit card, credit card, or bank account ("funding sources") to his or her PayPal account and code encryption safely allows users to make transactions over the computer with those funding options.[24] Code encryption is a method of security that sends a code containing the user's payment information from the originator (e.g., PayPal), to the recipient merchant.[25] This method of security is intended to keep a user's information out of the reach of everyone except for the intended recipient.[26] The user's information, however, is ultimately decrypted and stored in the recipient merchant's payment database.[27]

Once a user uploads payment information to PayPal, the user can transfer funds from one of the funding sources through his or her PayPal account to an authorized PayPal account held by another individual or merchant.[28] Users can also store funds from one of their funding sources in their PayPal accounts for convenience in making online purchases or executing quick transfers to other users.[29]

PayPal generally earns money in three ways. First, PayPal collects fees from merchants and other authorized businesses that utilize PayPal with every PayPal transaction.[30] Second, PayPal combines the money that users store in their personal PayPal accounts into pooled accounts in order to earn interest on those funds.[31] Instead of giving the

---

24. *See* Ed Grabianowski & Stephanie Crawford, *How PayPal Works*, How Stuff Works (Dec. 13, 2005), http://money.howstuffworks.com/paypal.htm (explaining how PayPal utilizes code encryption and also asserting how PayPal is considered to be a secure payment method).

25. *See* Andy Greenberg, *Hacker Lexicon: What is End-to-End Encryption?*, WIRED (Nov. 25, 2014, 9:00 AM), http://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/ (explaining how encryption works in a digital setting).

26. *Id.*

27. *See id.* (illustrating how the recipient stores and decrypts the data).

28. Grabianowski & Crawford, *supra* note 24.

29. *Id.*

30. *PayPal Merchant Fees: Current Rates for All Merchant Accounts*, PAYPAL https://www.paypal.com/us/webapps/mpp/merchant-fees (last visited Sep. 30, 2015). PayPal charges merchants a fee of 2.9% and $0.30 per transaction and PayPal offers deductions for non-profits and for businesses that subscribe to one of PayPal's merchant plans. *Id.*

31. Lenora Chu, *What PayPal Does With Your Money*, CNNMONEY (Feb. 26, 2008, 11:30 AM), http://money.cnn.com/2008/02/26/smbusiness/paypal_float.fsb/. PayPal generates an estimated at most $10 million per quarter from their pooling of funds into the corporate bank account. *Id.* However, users can get an interest return on their accounts if they enroll in the PayPal money market program. If enrolled, PayPal places the money in a money market fund managed by Barclay Global Investments and has an interest rate of 3.46%. *Id.*

interest back to the user, PayPal retains the interest earned.[32] Third, PayPal offers a heightened security feature for those willing to pay a fee.[33] A merchant can add on "Advanced Fraud Protection Services" for $10 per month plus $0.05 per transaction.[34]

B. Venmo

Venmo, launched in 2012,[35] is a payment service similar to PayPal, but geared almost exclusively toward paying with a mobile device.[36] Venmo is a mobile wallet, meaning that it is a storage space for digital versions of debit and credit cards held for making payments[37] that can be used with all internet-enabled mobile devices if a user downloads the free App.[38] Venmo processed $2.4 billion in person-to-person ("P2P") payments in 2014.[39] Venmo consolidates each user's funding sources into one wallet on their phone, or other internet-enabled mobile device like a tablet.[40] Users can link their debit card, credit card, or a United States bank account with their Venmo account.[41] Once the funding source is linked with the user's Venmo account, the user can add money to his or her Venmo balance or use Venmo to facilitate a transfer of funds from one of his or her funding sources to another user's Venmo account, or from his or her Venmo account to one of his or her bank accounts.[42] Venmo stores a user's funding information on its "bank grade

32. *Id.*

33. *See PayPal Merchant Fees: Current Rates for All Merchant Accounts*, *supra* note 30.

34. *Id.*

35. Jim Aramanda, *For the Record*, THE CLEARING HOUSE: BANKING PERSPECTIVE, Quarter 3 2015, at 8.

36. Felix Gillette, *Cash is for Losers!*, BLOOMBERG BUS. (Nov. 20, 2014), http://www.bloomberg.com/bw/articles/2014-11-20/mobile-payment-startup-venmo-is-killing-cash.

37. *Mobile Wallet Technology*, J.P. MORGAN CHASE PAYMENTECH https://www.chasepaymentech.com/mobile_wallet_technology.html (last visited Jan. 26, 2016).

38. *What is Venmo?*, VENMO HELP CTR. [hereinafter VENMO HELP CTR.], https://help.venmo.com/customer/portal/articles/1322558-what-is-venmo- (last updated July 2, 2015).

39. Aramanda, *supra* note 35.

40. *See* VENMO HELP CTR., *supra* note 38.

41. *Id.*

42. *Id.*

security system."[43]

Venmo's revenue generation model differs from PayPal's. Whenever a credit card or non-major debit card is the funding source for a user's Venmo account, the user must pay a 3% transaction fee, whereas it costs users nothing to use their debit card or bank account as a funding source.[44] As of now, Venmo is not an available payment method at the point of sale, in person or online, which drastically limits Venmo's current revenue model and market share.[45] Moreover, Venmo claims that it "does not typically receive interest on funds held for its users," although it does reserve the right to do so.[46]

C. Google Wallet and Android Pay

One of the mobile payment services that is poised to become Apple Pay's largest competitor is Google Wallet.[47] Although some of the features of Google Wallet, specifically the transfer of money at the point-of-sale, are being transferred to Android Pay,[48] Google Wallet will maintain many features, and together the two Alphabet-owned[49] Apps will be competitive with Apple Pay.[50] Much like Venmo, Google Wallet

---

43. *Security*, VENMO, https://venmo.com/about/security/ (last visited Jan. 26, 2016).

44. Gillette, *supra* note 36.

45. *Id.*

46. *User Agreement* at (B)(1)(h)(ii), VENMO (Jan. 27, 2016), https://venmo.com/legal/us-user-agreement/.

47. *See* Chris Hoffman, *Google Wallet v. Apple Pay: What You Need to Know*, HOW-TO GEEK (Nov. 16, 2014), http://www.howtogeek.com/201870/google-wallet-vs.-apple-pay-what-you-need-to-know/ (recognizing the attention Apple Pay has received but also other growing mobile payment methods, especially Google Wallet).

48. Andrew Martonik, *What's the Difference Between Android Pay and the New Google Wallet?* ANDROIDCENTRAL (Sep. 17, 2015, 12:45 PM), http://www.androidcentral.com/whats-difference-between-android-pay-and-new-google-wallet. Android Pay is a separate mobile application and is available for free download on non-Apple smartphones. Android Pay is intended to be used in combination with Google Wallet. Android Pay is intended for use at a point of sale, whereas Google Wallet in itself is intended for person-to-person transfers. *Id.*

49. *See* Heather Kelly, *Meet Google Alphabet – Google's New Parent Company*, CNN MONEY (Aug. 11, 2015, 6:01 PM), http://money.cnn.com/2015/08/10/technology/alphabet-google/ (explaining how Alphabet is now Google's parent company, meaning that all companies that Google owns are now owned by Alphabet).

50. Andrew Martonik, *Google Wallet Isn't Being Completely Replaced by Android Pay, But Big Changes are Coming*, ANDROID CENTRAL (May 28, 2015, 9:36 PM), http://www.androidcentral.com/google-wallet-isnt-being-replaced-android-pay-big-changes-are-coming. Some of the features of Google Wallet are in the process of being transferred over to Android Pay. *Id.* Although Google Wallet will still exist, the main reason it will be

is a mobile wallet that is intended to store all of a user's funding sources in one convenient location.[51] Google Wallet is available on Android and Apple mobile devices, so long as a user downloads the free App.[52] In Google Wallet, unlike PayPal or Venmo, a user can store more than just credit cards, debit cards, or bank account information.[53] Users can also store gift cards or loyalty cards, theoretically eliminating the need for a physical wallet for payment purposes.[54] Google Wallet is similar to PayPal in that a user can also store funds in a Google Wallet account for ease of payment.[55]

When a user stores funds in a Google Wallet account, Google Wallet issues the user, if he or she chooses, a *physical* Google Wallet debit card.[56] This is a bit counterintuitive to the purpose of a mobile payment service. Users can use the physical Google Wallet card to pay for goods and services just like a user currently uses a debit card.[57] A Google Wallet account can be used multiple ways. First, through Android Pay, it can be used to ease the transfer of funds between users and a merchant wherever Google Wallet or Android Pay is accepted at the point of sale by reducing the need for a user to carry a physical wallet or sign receipts.[58] Second, users can also use a Google Wallet account to transfer funds to anybody in the United States who has a Google Wallet or Gmail account.[59]

Google Wallet has partnered with MasterCard so that users can use their physical Google Wallet card anywhere that debit MasterCard is accepted.[60] Furthermore, users can utilize Google Wallet's mobile payment method anywhere that MasterCard PayPass, a form of payment powered by MasterCard at the point-of-sale that utilizes Near-Field

---

the main competitor to Apple Pay is its partnership with Android Pay.

51. *Frequently Asked Questions*, GOOGLE WALLET [hereinafter GOOGLE WALLET], https://www.google.com/wallet/faq.html (last visited Aug. 26, 2015).

52. *Id.*

53. *Id.*

54. *Id.*

55. *Id.*

56. *Id.*

57. *Id.*

58. Martonik, *supra* note 48.

59. GOOGLE WALLET, *supra* note 51.

60. *See id*. (explaining how the Google Wallet Card can be used anywhere Debit MasterCard is accepted).

Communication ("NFC")[61] technology with various devices,[62] is accepted.[63] Since Google Wallet is available on multiple platforms and appears, because of Google's brand recognition,[64] to reach the widest audience, one would guess that it is incredibly profitable. This is not true.[65]

Google Wallet, unlike competitors, does not use transaction fees as a revenue generator.[66] Instead, Alphabet collects a user's purchasing data and uses that data to drive advertising revenue by increasing the effectiveness of targeted advertisements to individual users.[67] Google Wallet also makes money by charging users a fee to put funds into their Google Wallet account.[68] Given the immense amount of credit card use, especially considering the MasterCard partnership,[69] Google Wallet is missing the chance to collect large sums of money in the form of transaction fees.[70] Whether Google Wallet will prove to be a financially viable business model, or if the service will have to begin collecting transaction fees in pursuit of profitability, remains to be seen.[71]

---

61. "Near field communication, abbreviated NFC, is a form of contactless communication between devices like smartphones or tablets. Contactless communication allows a user to wave the smartphone over a NFC compatible device to send information without needing to touch the devices together or go through multiple steps setting up a connection." *About Near Field Communication*, NEARFIELDCOMMUNICATION.ORG, http://www.nearfieldcommunication.org/about-nfc.html (last visited Jan. 26, 2016).

62. Vaseem Khan, *MasterCard's PayPass: Has it Really Made a Dent in the Contactless Payments Market?*, LET'S TALK PAYMENTS (Oct. 16, 2013), http://letstalkpayments.com/paypass-mastercards-answer-to-provide-a-contactless-payment-platform/.

63. GOOGLE WALLET, *supra* note 51.

64. *See* Felix Richter, *1.17 Billion People Use Google Search*, STATISTA (Feb. 12, 2013), http://www.statista.com/chart/899/unique-users-of-search-engines-in-december-2012/ (illustrating the broad reach of Google which includes more than 1 billion users per month).

65. Mark Milian & Ari Levy, *Google Wallet is Leaking Money*, BLOOMBERG BUS. (June 6, 2013), http://www.bloomberg.com/bw/articles/2013-06-06/google-wallet-is-leaking-money.

66. *Id.*

67. *Id.*

68. *Wallet Help*, GOOGLE WALLET, https://support.google.com/wallet/answer/6285493?hl=en (last visited Feb. 12, 2016).

69. *See* Kahn, *supra* note 62 (explaining how MasterCard had issued 92 million PayPass cards and 310,000 acceptance points).

70. Milian & Levy, *supra* note 65.

71. Google debuted Android Pay on September 10, 2015. It is too early to see how this will impact Apple Pay. *See* Martonik, *supra* note 48. However, Alphabet has already self-reported to FinCEN under the name Google Payment Corp. MSB Registrant Search Web Page: Google Payment Corp., U.S. DEP'T OF THE TREASURY: FIN. CRIMES ENFORCEMENT NETWORK, https://www.fincen.gov/financial_institutions/msb/msbstateselector.html (last

D. The Future, Scope, and Size of the Mobile Payment Industry

Convenience is the main draw of electronic payment services, especially with regards to mobile payments.[72] Various companies are all attempting to achieve a similar goal of eliminating the need for consumers to carry cash or physical payment cards by enabling them to conduct all financial transactions from their mobile phones.[73] The mobile payment industry is already large,[74] but it is poised for additional growth in the near future.[75] Mobile payment services will revolutionize the way people pay for goods and services on a daily basis.[76] A recent study found that 87% of adults in America said that they either owned or had regular access to a mobile phone and 71% of those phones are internet-enabled smartphones.[77] Roughly speaking, this means that 62% of adults in America either own, or have regular access to, an internet-enabled smartphone.[78] Although a poll conducted at the end of 2013 showed that only 8% of people claimed to have used a mobile payment service that number is quickly climbing.[79] One year later, an identical poll rendered a much different result: 40% of Americans reported having used a mobile payment service.[80] Clearly, this is a growing industry and there are various methods currently being employed in an effort to make this industry profitable.[81]

---

visited Jan. 26, 2016).

72. *Mobile Wallet Technology*, *supra* note 37.

73. *See* Drozdowski et al., *supra* note 17 (explaining the goal of the mobile payment marketplace).

74. *Mobile Payments in the United States from 2014 to 2019, By Segment (In Million U.S. Dollars)*, STATISTA http://www.statista.com/statistics/312492/mobile-payments-in-the-united-states-by-segment/ (last visited Jan. 26, 2016). "In 2018, mobile in-person payments are projected to reach 23.47 billion U.S. dollars, up from 3.73 billion U.S. dollars in 2014." *Id.*

75. *Id.*

76. Drozdowski et al., *supra* note 17.

77. BD. OF GOVERNORS OF THE FED. RES. SYS., CONSUMERS AND MOBILE FIN. SERVS. 1 (2015).

78. *See id.* (multiplying the percentage of people who own or have regular access to a cell phone by the percentage of those phones that are internet-enabled smartphones).

79. *Mobile Payment Statistics*, NASDAQ (Mar. 30, 2015, 8:00 AM), http://www.nasdaq.com/article/mobile-payment-statistics-cm460412.

80. *Id.*

81. Drozdowski et al., *supra* note 17.

III. APPLE PAY

Apple Pay differs from these other mobile payment services in many ways. Apple Pay is only available on Apple mobile devices, specifically the iPhone 6 model or newer and the Apple Watch.[82] Apple has sold over 180 million Apple Pay-enabled iPhones,[83] but Apple will not disclose how many users regularly use Apple Pay or how much money Apple Pay handles.[84] Apple claims that it only stores an encrypted version of a user's debit or credit card information on its secure servers.[85] Using NFC technology, Apple Pay transmits funds, via electronic tokens, from the user's mobile device to the merchant's Apple Pay compatible point-of-sale device.[86] The user then authenticates the purchase with his or her fingerprint or personal security code.[87]

Although users can store credit and debit card information on Apple Pay, a user cannot store money in an Apple Pay account.[88] This inability to store money in an account is an important difference between Apple Pay and other forms of mobile payment. The inability to store money is part of the reason that Apple Pay claims to be so secure.[89] The idea behind this claim of superior security is that because the funds are not on the user's device, a thief cannot directly withdraw funds with only access to the device.[90] The other reason why Apple Pay claims to be

---

82. Press Release, Nat Kerris & Laura Newell, Press Contacts, Apple, Apple Pay Set to Transform Mobile Payments Starting October 20 (Oct. 16, 2014) (Apple Pay is also available for customers shopping online with iPad Air 2 and iPad Mini 3 or newer).

83. *Apple Pay Adoption: The Falling Side of the Bell Curve*, PYMNTS.COM (Aug. 5, 2015), http://www.pymnts.com/in-depth/2015/apple-pay-adoption-the-falling-side-of-the-bell-curve/.

84. *New Data Shows Apple Pay Still Stuck in the Mud*, PYMNTS.COM (Oct. 6, 2015), http://www.pymnts.com/news/2015/new-data-shows-apple-pay-still-stuck-in-the-mud/.

85. *Apple Pay Security and Privacy Overview*, APPLE [hereinafter *Apple Pay Security*], https://support.apple.com/en-us/HT203027 (last modified Oct. 28, 2015).

86. *Id.*

87. *Apple Pay Security*, *supra* note 85.

88. *Id.*

89. Cole, *supra* note 12.

90. *Apple Pay Security*, *supra* note 85. However, this may change if and when Apple Pay is enabled for use at ATMs. *See* Josh Constine, *Apple Pay is Coming to ATMs From Bank of America and Wells Fargo*, TECH CRUNCH (Jan. 28, 2016), http://techcrunch.com/2016/01/28/apple-pay-atm/#.akr41zx:HCN6 (explaining how banks are in the process of integrating mobile payment services into their ATMs). However, this would expand the already present security issue of a thief using a stolen card on Apple Pay, except now the thief would have direct fund access. *See infra* note 200.

secure is its use of tokenization.[91] Tokenization is a mechanism by which a unique sixteen-digit code, or token, is created every time Apple Pay is used at a point-of-sale.[92] When the transaction is initiated, the token is transferred to the merchant instead of the user's debit or credit card information, which ensures that the user's debit or credit card information is not stored in a merchant's database.[93] Considering that Apple Pay's business is more akin to facilitating the ordering of fund transfers, as opposed to quasi-banking (when funds may be stored in a user's account) like other mobile payment services, they must also have a different business model.[94]

Apple Pay's current revenue generation model is surprisingly lucrative.[95] Apple charges credit and debit card *issuers* who accept Apple Pay a 0.15% fee, or 15 basis points.[96] This 0.15% fee that Apple collects from the credit and debit card issuers comes from a variety of sources.[97] There are fees for tokenization that the merchant's bank must pay to the card manufacturer which factor into Apple's 0.15%.[98] There are also fees on credit card interchanges between the user's bank and the merchant's bank.[99] When a consumer purchases an item from a merchant using a card that has been uploaded to Apple Pay, the card issuing company charges the merchant's bank a fee, a percentage of the amount spent by the consumer to the consumer's bank, known as the interchange fee.[100] The merchant's bank will then charge the merchant a "discount fee" on the consumer's purchase in order to regain what they have lost and turn a profit.[101] Apple Pay collects from the interchange fee what the

---

91. *Apple Pay Security*, *supra* note 85.

92. *How Apple Pay Works and Why It Matters to Developers*, CLOVER DEVELOPERS BLOG, (Sep. 9, 2014) http://clover-developers.blogspot.com/2014/09/apple-pay.html.

93. Cole, *supra* note 12.

94. *See* WIGLEY + COMPANY SOLICITORS, HOW DOES APPLE MAKE MONEY FROM APPLE PAY? 3 (2015), http://www.wigleylaw.com/assets/Uploads/How-does-Apple-make-money-from-Apple-Pay.pdf#page=4 (explaining how Apple Pay has a unique business model).

95. *Id.* at 4.

96. *Apple Pay's Business Model Blues*, PYMNTS.COM (Apr. 17, 2015, 6:15 AM) [hereinafter PYMNTS], http://www.pymnts.com/in-depth/2015/apple-pays-business-model-blues/#.VdN_m_lViko.

97. *Id.*; WIGLEY + COMPANY SOLICITORS, *supra* note 94 at 4.

98. WIGLEY + COMPANY SOLICITORS, *supra* note 94 at 4.

99. *Apple Pay's Business Model Blues*, *supra* note 96.

100. *In re* Visa Check/MasterMoney Antitrust Litig., 280 F.3d. 124, 130 n.2 (2d Cir. 2001).

101. *Id.*

merchant's bank pays to the card issuing bank when Apple Pay is used and this factors into Apple's 0.15% fee.[102] The two entities that Apple does not charge directly are the individual user and the merchant who enables the Apple Pay transaction.[103] Essentially, the merchant pays nothing directly to Apple, however, the merchant will have to pay their bank an additional fee on every Apple Pay transaction the merchant processes.[104]

IV. SECURITY CONCERNS AND THE CURRENT REGULATORY ENVIRONMENT

The FDIC has declared that "to date, no federal laws or regulations specifically govern mobile payments."[105] This statement should cause some concern. How can an industry that processes billions of dollars per year in the U.S. alone and used by 40% of Americans be unregulated?[106] There are several reasons. The mobile payment service industry is relatively new.[107] Not only is it difficult to predict how big the mobile payment industry may become, but it is even more difficult to predict which platform will dominate the industry.[108] Many would argue that there is no sense in creating platform-specific regulations when the mobile payment market is so young and a true industry leader has yet to emerge.[109] Another reason that there is no specific mobile payment regulation is because many mobile payment services have voluntarily subjected themselves to the current regulatory regimes of the Electronic Funds Transfer Act ("EFTA"), the Gramm-Leach-Bliley Act ("GLBA"), and the Bank Secrecy Act ("BSA") by registering with the government.[110] Simply put, the government has employed a wait-and-see mentality and the wisdom of such a stance has yet to be called into question.

---

102. *Apple Pay's Business Model Blues*, *supra* note 96.

103. *About Apple Pay for Merchants in the US*, APPLE, https://support.apple.com/en-us/HT204274 (last visited Sep. 30, 2015); WIGLEY + COMPANY SOLICITORS, *supra* note 94 at 4.

104. WIGLEY + COMPANY SOLICITORS, *supra* note 94 at 3-4 (explaining how a merchant's bank will pass Apple's charges to the individual merchants).

105. Drozdowski et al., *supra* note 17.

106. *Mobile Payment Statistics*, *supra* note 79.

107. Drozdowski et al., *supra* note 17.

108. *Id.*

109. *Id.*

110. Rubenfeld, *supra* note 10.

A. The EFTA

The EFTA establishes rules for electronic fund transfers involving consumers.[111] The EFTA applies to "any electronic fund transfer that authorizes a financial institution to debit or credit a consumer's account. Generally, this part applies to financial institutions."[112] Although the EFTA does not provide a definition for "financial institution," it defines an "account" as "a demand deposit (checking), savings, or other consumer asset account . . . held directly or indirectly by a financial institution."[113] Therefore, mobile payment providers who store users' funds in an account will likely be considered financial institutions.[114] Furthermore, the EFTA defines an "electronic fund transfer" as "any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account."[115] The EFTA requires businesses to disclose several pieces of information to their consumers including a telephone number and an address where consumers can reach a business.[116] Businesses must also disclose their confidentiality standards.[117] Currently, Apple only provides users with a customer help telephone number.[118] Regulation stemming from the EFTA requires subject businesses to document certain records such as individual transaction receipts or periodic statements that set forth individual transactions.[119] The major consequence of EFTA regulation is the liability of a business to a consumer for fraudulent activity by virtue of limiting the consumer's liability.[120] If a consumer reports fraudulent activity within two days of when it occurred, the consumer is liable for a maximum of $50 of the fraud; if reported within sixty days, the consumer

111. Electronic Funds Transfer Act, 15 U.S.C. § 1693 (2012), Electronic Fund Transfer (Regulation E), 12 C.F.R. § 1005.1 (2015).

112. *Id.* § 1005.3(a).

113. *Id.* § 1005.2(b)(1).

114. *See id.*

115. *Id.* § 1005.3(b).

116. *Id.* § 1005.7(b)(2).

117. *Id.* § 1005.7(b)(8).

118. *See Apple Pay Security*, *supra* note 85 (providing a customer support phone number for customer contact on this page with no address or other disclosures are available).

119. 12 C.F.R. § 1005.7(b)(6).

120. *Id.* § 1005.6(b).

liability jumps to a maximum of $500.[121]

Currently, Apple Pay fits within an exception to the EFTA even though other mobile payment services are covered.[122] Venmo, PayPal, and Google Wallet are all subject to the EFTA because they actually store funds in users' accounts.[123] Furthermore, Google Wallet issues users a physical debit card with which to complete transactions.[124] Apple Pay's platform does not fall under the categories of platforms governed by the EFTA for a couple of reasons.[125] First, Apple does not store user's funds in an account like its competitors.[126] Because of this, even if Apple Pay is considered an electronic fund transfer service, it must be considered an electronic fund transfer service provider that does not hold the user's account, which is one of the exceptions from being regulated under the EFTA.[127] Second, only a user's card information, not actual funds, are ever in Apple's possession, even when the funds are transferred from the user to the merchant via Apple Pay.[128] Apple Pay merely simplifies the transaction between the user and the merchant at the point-of-sale, but there is no actual transfer of money to or by Apple.[129]

Even when a business does not hold a user's account, the business is subject to EFTA regulation if the business also "issues a debit card (or other access device) that the consumer can use to access the consumer's account held by a financial institution" and the business "[h]as no agreement with the account-holding institution regarding such access."[130] Apple Pay's platform falls short of both requirements.[131]

---

121. *Id.*

122. *See id.* § 1005.14(a) (illustrating the exceptions to being regulated under the Electronic Funds Transfer Act).

123. *Id.* § 1005.2(b)(1) (defining account for purposes of regulation).

124. *Your Wallet Card*, GOOGLE: WALLET HELP, https://support.google.com/wallet/answer/6285510?hl=en (last visited Nov. 14, 2015).

125. Rubenfeld, *supra* note 10.

126. *Id.*

127. *See* 12 C.F.R. § 1005.14(a) (illustrating the exceptions to being regulated under the Electronic Funds Transfer Act).

128. *iOS Software User Agreement (B)(3)*, APPLE, http://images.apple.com/legal/sla/docs/iOS81.pdf (last visited Sep. 30, 2015).

129. Rubenfeld, *supra* note 10.

130. 12 C.F.R. § 1005.14(a).

131. *See* Rubenfeld, *supra* note 10 (illustrating how Google Wallet is unique in that it issues users a physical debit card); Malarie Gokey, *Here are All the Places that Support Apple Pay: Australia Could be Next, if Banks Agree*, DIGITAL TRENDS (Aug. 18, 2015), http://www.digitaltrends.com/mobile/apple-pay-partners-news/.

Apple Pay does not issue debit cards like Google Wallet.[132] However, competitors can arguably assert that since Apple Pay is only accessible through an Apple mobile device, Apple does indeed issue the "access device" that the user can use to access the user's account. Apple Pay, however, does not allow users to fully access their accounts, but to merely use Apple Pay to order a transfer of money from a user's funding account to a merchant.[133] However, this point is moot since Apple clearly does not fall under the second provision of having no agreement with the account-holding institutions.[134]

Apple has agreements with every account-holding institution that allows its users to upload their account information to Apple Pay.[135] Currently, this list includes the four major credit card companies—Visa, MasterCard, Discover, and American Express—as well as over 400 banking institutions across the United States.[136] Apple currently has agreements with institutions that make up 90% of the credit card transactions in the United States.[137] Whether or not Apple Pay is regulated by the EFTA may not seem like a pertinent issue at the moment, but if there is a security breach with Apple Pay, users will want to know that Apple Pay has been documenting its activity, as currently required of other institutions subject to the EFTA. Since the federal government acts as both a merchant and institution in its use of Apple Pay,[138] the EFTA should be expanded to include Apple Pay so that the government, and ultimately tax payers, are not forced to foot the bill for any fraudulent activity that may occur through Apple Pay.[139]

B. The GLBA

The GLBA requires financial institutions to explain their information-sharing practices to their customers as well as safeguard sensitive data.[140] This includes both the Interagency Guidelines

132. Rubenfeld, *supra* note 10.
133. *Id.*
134. Gokey, *supra* note 131.
135. *Id.*
136. *Id.*
137. *Id.*
138. Higgins & Dexheimer, *supra* note 3.
139. *Id.*; *See also* 12 C.F.R. § 1005.6(b).
140. FED. TRADE COMM'N – GRAMM-LEACH-BLILEY ACT, https://www.ftc.gov/tips-

Establishing Standards for Safeguarding Customer Information ("Interagency Guidelines") adopted by the federal financial regulatory agencies, and Safeguards Rule promulgated by the Federal Trade Commission ("FTC").[141] Mobile payment services do not have to follow the Interagency Guidelines because they are not banks subject to the GLBA.[142] However, most mobile payment services are subject to the Safeguards Rule.[143]

The Safeguards Rule requires financial institutions to develop a written information security plan that describes the program(s) they use to protect customer information.[144] An adequate information security program includes five elements.[145] First, the financial institution must designate an employee to coordinate the program.[146] Second, the program must "[i]dentify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of [such] safeguards."[147] Third, the program must "[d]esign and implement information safeguards to control risks" identified through regular assessments, and regularly test or monitor "the effectiveness of safeguards' key controls."[148] Fourth, the program must oversee service providers, including "taking reasonable steps" to retain "providers that are capable of maintaining appropriate safeguards" and contractual provisions requiring such safeguards.[149] Lastly, the program must evaluate and adjust the "program in light of testing and monitoring," material changes to the business, or other circumstances with a material impact on the information security program.[150]

The definition of a financial institution covered by the Safeguards

---

advice/business-center/privacy-and-security/gramm-leach-bliley-act (last visited Nov. 17, 2015).

141. THE CLEARING HOUSE, ENSURING CONSISTENT CONSUMER PROTECTION FOR DATA SECURITY: MAJOR BANKS VS. ALTERNATIVE PAYMENT PROVIDERS 12 (2015).

142. *Id.* at 15.

143. *Id.*

144. Standards for Safeguarding Customer Information, 16 C.F.R. § 314.3(a) (2015).

145. *Id.* § 314.4.

146. *Id.* § 314.4(a).

147. *Id.* § 314.4(b).

148. *Id.* § 314.4(c).

149. *Id.* § 314.4(d).

150. *Id.* § 314.4(e).

Rule is broad.[151] A financial institution is defined as an institution that is "significantly engaged in financial activities."[152] Although a mobile payment service provider is nowhere to be found in the regulation's examples, most mobile payment platforms are involved in the business of transferring money.[153] Transferring money is a financial activity that is directly referred to in the regulations as being covered by the Safeguards Rule.[154] Mobile payment services can be said to transfer money if they are analogous to a money wiring service.[155] Money wiring services transfer funds from P2P, much like PayPal, Venmo, and Google Wallet.[156] Therefore, mobile payment services analogous to money wiring services should be classified as financial institutions under the Safeguards Rule.[157]

As it stands currently,[158] Apple Pay is not subject to the Safeguards Rule because there is a factual difference between a typical money transfer service and Apple Pay.[159] Not only does Apple Pay never have access to the funds being transferred, but Apple Pay does not resemble a money wiring service in that it does not transfer funds to other individuals.[160] It is best to think of Apple Pay as a digital counter upon which the cash register sits. If a person places his or her debit card on the counter and then the merchant takes the card for payment, you would not say that the counter transferred the funds from the card to the merchant. Apple Pay is the digital equivalent.

Although Apple Pay does not have access to a user's funds, it does have access to much of a user's sensitive information.[161] The GLBA

---

151. Privacy of Consumer Financial Information, 16 C.F.R. § 313.3(k)(1) (2015).

152. *Id.*

153. Drozdowski, et al., *supra* note 17.

154. 16 C.F.R. § 313.3(k)(2).

155. *See id.* § 313.3(k)(2)(vi) ("A business that regularly wires money to and from consumers is a financial institution because transferring money is a financial activity referenced in section 4(k)(4)(A) of the Bank Holding Company Act and regularly providing that service demonstrates that the business is significantly engaged in that activity.").

156. Grabianowski & Crawford, *supra* note 24; VENMO HELP CTR., *supra* note 38; GOOGLE WALLET, *supra* note 51.

157. *See* 16 C.F.R. § 313(k)(2)(vi).

158. *See* Don Reisinger, *Is Peer-to-Peer Apple Pay's Next Frontier?*, TIME, INC.: FORTUNE (Dec. 21, 2015, 7:30 PM), http://fortune.com/2015/12/01/apple-pay-peer-to-peer/ (showcasing rumors that Apple Pay has been developing a P2P service, however, at the time of publication, this has not been verified by Apple).

159. Rubenfeld, *supra* note 10.

160. *Id.*

161. iOS Software User Agreement (B)(3), *supra* note 128.

should be expanded so that all mobile payment services that have access to a customer's information, including Apple Pay, must implement a safeguard program.[162] Given that the federal government has expressly authorized citizens to place their information in the hands of Apple Pay, measures must be taken to protect that information.[163]

C. The BSA

The BSA established the U.S. Treasury Financial Crimes Enforcement Network ("FinCEN").[164] Businesses that perform certain functions must register with FinCEN as a Money Service Business ("MSB").[165] MSBs encompass several subsets of businesses, including issuers, sellers, or redeemers of money orders or traveler's checks; providers or sellers of prepaid access (cards); check cashers; and dealers in foreign exchange.[166] A different subset of MSBs, and the subset that mobile payment services fall under, is Money Transmittal Businesses ("MTBs").[167]

The courts have provided little guidance on what constitutes an MTB, particularly in regards to electronic payments. In *United States v. E-Gold, Ltd.*,[168] the United States District Court for the District of Columbia held that Congress intended a plain English reading of the statute, particularly the requirements for being an MTB.[169] The statute defines an MTB as any business which:

Provides check cashing, currency exchange, or money transmitting or remittance services, or issues or redeems money orders, travelers' checks, and other similar instruments or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional

---

162. *See* The Gramm-Leach-Bliley Act, 15 U.S.C. § 6809, 16 C.F.R. § 313.3(k) (2015) (listing the types of businesses that are deemed to need safeguard programs).

163. Higgins & Dexheimer, *supra* note 3.

164. Bank Secrecy Act, 31 U.S.C. § 5330 (2012), 31 C.F.R. § 1010.100(s) (2015).

165. 31 C.F.R. § 1010.100(ff).

166. *Id.*

167. 31 U.S.C. § 5330(d)(1)(A).

168. United States v. E-Gold, Ltd., 550 F. Supp. 2d 82, 92–93 (D.D.C. 2008).

169. *Id.*

financial institutions system.[170]

The *E-Gold* case primarily highlighted how electronic payment systems can be considered MTBs despite not dealing directly with cash currency.[171]

An MSB that is registered with FinCEN is required to do several things. First, all MSBs must establish a written anti-money laundering ("AML") program.[172] An AML program includes internal policies, procedures, and reasonably designed controls to guard against the firm being used for money laundering or terrorist financing.[173] An adequate program also includes an officer for oversight, as well as continuing training and auditing.[174] Second, MSBs are required to keep a record of the transmittal of users' funds.[175] Lastly, MSBs are required to report suspicious activity in the form of a suspicious activity report ("SAR").[176]

Apple is not currently registered as an MSB like its competitors PayPal, Venmo, Google Wallet, and Android Pay.[177] Apple does not fall under the category of MTBs.[178] Given a plain-English reading of the definition of an MSB described in *United States v. E-Gold*, one can see the arguments on Apple's side.[179] First, Apple has always prided itself on its product which simply *enables* the facilitation of money transfers, but does not actually transfer money, thereby keeping it out from under the statute.[180] Second, what Apple Pay does cannot be considered "facilitating," as it is doing nothing more than providing the digital counter space upon which the transaction takes place. The government would not regulate the physical counter that the cash register sits on, so a digital counter is no different.

Because Apple Pay is not currently registered as an MSB, it is not

---

170. 31 U.S.C. § 5330(d)(1)(A).

171. *E-Gold, Ltd.*, 550 F. Supp. 2d at 92–93.

172. 31 C.F.R. § 1022.210(a) (2015).

173. *Anti-Money Laundering ("AML") Programs*, NAT'L FUTURES ASS'N, https://www.nfa.futures.org/NFA-faqs/compliance-faqs/anti-money-laundering/index.HTML#q1 (last visited Jan. 7, 2016).

174. *Id.*

175. Bank Secrecy Act, 31 U.S.C. § 5330 (2012), 31 C.F.R. § 1010.410(e) (2015).

176. 31 C.F.R. § 1020.320(m).

177. Rubenfeld, *supra* note 10; *see also MSB State Selector – Apple*, FINCEN, https://www.fincen.gov/financial_institutions/msb/msbstateselector.html (last visited Jan. 10, 2016).

178. Rubenfeld, *supra* note 10.

179. United States v. E-Gold, Ltd., 550 F. Supp. 2d 82, 92–93 (D.D.C. 2008).

180. iOS Software User Agreement, *supra* note 128.

required to have an AML program.[181] Furthermore, it is not required to file SARs.[182] Although a data breach in itself does not require a SAR, the moment the breach reaches the $2,000 minimum required by FinCEN, a SAR must be filed.[183] By not registering with FinCEN, Apple Pay is saving money by avoiding standard security practices of creating an AML program, training employees on that program, and ensuring that the AML program is effective.[184]

D. Securing the Mobile Payment Industry

The issue of security is at the heart of any new industry-leading technology, especially technology regarding money transmission.[185] Financial institutions want to know that their consumers' money is secure in someone else's hands and users want to know that if there is a large-scale data breach or identity theft, they will have recourse for the recovery of their funds.[186] Users also have privacy concerns when it comes to the government, particularly in light of recent issues regarding the practices of the National Security Agency, some of which have been condemned and outlawed.[187] Regulatory schemes such as the EFTA, the GLBA, and the BSA address security issues and set baselines for what users can expect from their financial companies, including the federal government, regarding the security of their funds.[188]

With such a widespread technology as Apple Pay not subject to these regimes, users have little assurance that their money and information are safe. Furthermore, with the federal government submitting itself to Apple Pay as both a merchant and card-issuing

181. The Bank Secrecy Act, 31 U.S.C. § 5330 (2012), 31 C.F.R. § 1022.210(a) (2015).

182. *Id.* § 1020.320.

183. *Id.*

184. *Id.*

185. *See* Madden & Rainie, *supra* note 9 (illustrating a very low confidence rate in internet-based technology companies, and a low confidence rate in current credit card companies).

186. *See* Sorkin, *supra* note 8 (showing how financial institutions are very wary of the security risk present with Apple Pay, but will not speak up "for fear of upsetting their company's relationship with Apple").

187. Madden & Rainie, *supra* note 9.

188. *See generally* The Electronic Funds Transfer Act, Regulation E, 15 U.S.C. § 1693 (2012), 12 C.F.R. § 1005.1(b) (2015); The Gramm-Leach-Bliley Act, 15 U.S.C. § 6809 (2012), 16 C.F.R. § 314.3(A) (2015); The Bank Secrecy Act, 31 U.S.C. § 5330 (2012), 31 C.F.R. § 1010.100(s) (2015).

institution,[189] government funds may now be the subject of theft.[190] Apple Pay claims that users have no need to worry about the security of their finances.[191] Apple Pay even claims, in advertisements as recent as fall of 2015, to be more secure than a credit card transaction.[192] To grasp what exactly Apple is claiming,[193] a look at the current state of security in the credit card industry is important.

E. Current Security Measures in the Credit Card World

In 2015, the United States adopted, under the leadership of the major credit card companies, "chip and PIN" technology for nearly all credit and debit cards, completing the switch from the magnetic strip cards that had been in use in the United States for many years.[194] The most important difference between magnetic strip card technology and "chip and PIN" card technology is the storage location of the user's financial data.[195] With magnetic strip card technology, the user's information is stored within the merchant's database.[196] Storing all of this information in one database can be incredibly problematic from a security standpoint because all the information is centrally located and

189. Higgins & Dexheimer, *supra* note 3.

190. *See* Yan, *supra* note 7 (illustrating how Apple Pay can be used in theft).

191. APPLE PAY OVERVIEW, www.apple.com/apple-pay/ (last visited Sept. 12, 2015).

192. *See id.* ("Every time you hand over your credit or debit card to pay, your card number and identity are visible, and swiping your card triggers an exchange of information. With Apple Pay, instead of using your actual credit and debit card numbers when you add a card, a unique Device Account Number is assigned, encrypted, and securely stored in the Secure Element, a dedicated chip in iPhone, iPad, and Apple Watch. When you make a purchase, the Device Account Number, along with a transaction-specific dynamic security code, is used to make your payment. So your actual credit or debit card numbers are never shared by Apple with merchants or transmitted with payment. And unlike credit cards, on iPhone and iPad every payment requires Touch ID or a passcode, and Apple Watch must be unlocked — so only you can make payments from your device").

193. *Id.*

194. *See* Max Eddy, *Chip and PIN Cards More Secure than Swipe Cards, Also Pretty Awful*, PCMAG: SECURITYWATCH (Aug. 07, 2014, 7:48 PM), http://securitywatch.pcmag.com/hacking/326213-chip-and-pin-cards-more-secure-than-swipe-cards-also-pretty-awful (showcasing how banks initiated the switch to Chip and PIN cards in the United States starting in 2015).

195. *EMV Cards are Proven to Reduce Fraud*, GEMALTO, http://www.gemalto.com/emv/fraud (last visited Feb. 12, 2016).

196. David Dayen, *Your Credit Card Has A Dangerous Flaw that the Banks Refuse to Fix*, NEW REPUBLIC (Jan. 16, 2014), https://newrepublic.com/article/116236/credit-card-magnetic-stripes-are-putting-you-risk-identity-theft.

only protected by the security provided by the merchant.[197] This longstanding flaw was exposed on an enormous scale in 2013, when a group of hackers stole the information of over forty million Target customers.[198]

"Chip and PIN" cards address this issue. With a "chip and PIN" card, the user's information is stored on the card chip and the merchant only accesses a one-time code of the user's information when the user's PIN is entered.[199] While it is still possible for hackers to glean information from individual cards or card readers that they have stolen or tampered with, the widespread security threat is minimized because the consumer's information is spread out among the individual cards as opposed to being aggregated in a single database location.[200]

F. Apple Pay's Security and Tokenization Technology

Apple Pay claims to be more secure than a "chip and PIN" credit card transaction because Apple Pay utilizes "tokenization."[201] Tokenization creates a unique code or "token" every time an individual utilizes Apple Pay to transfer money from the user's bank account or credit card to a merchant.[202] This method means that the merchant does not have access to, nor does it store, any of the user's actual bank or credit card information in its system at any time.[203]

A huge hole still resides in Apple Pay's security profile. Apple Pay makes it easy to load a debit or credit card onto an iPhone, meaning that when a physical credit card is lost or stolen, it is very easy for a thief to load it onto his or her iPhone to use with Apple Pay, as opposed to trying to use a stolen card in a store where many merchants require a photo ID to use a credit card.[204] In some instances, all a user has to do is enter in the card number, expiration date, and three or four digit

197. *See id.*; *See also* Miles Parks, *Target Offers $10 Million Settlement in Data Breach Dispute*, NPR: THE TWO-WAY (Mar. 19, 2015, 10:45 AM), http://www.npr.org/sections/thetwo-way/2015/03/19/394039055/target-offers-10-million-settlement-in-data-breach-lawsuit.

198. Parks, *supra* note 197.

199. Eddy, *supra* note 194.

200. *EMV Cards are Proven to Reduce Fraud*, *supra* note 195.

201. Rubenfeld, *supra* note 10.

202. *Id.*

203. *Id.*

204. Yan, *supra* note 7.

verification code to upload the card to Apple Pay.[205] There have even been cases where thieves have used stolen credit cards that they uploaded to Apple Pay to purchase items from an Apple store, illustrating, in an ironic fashion, that there are still severe security flaws to be sorted out by Apple.[206] One study estimates that up to six percent of purchases made with Apple Pay were fraudulent,[207] a rate sixty times higher than average credit card fraud rates.[208]

Apple admits that the ease of loading a card onto an iPhone is a threat to security. However, it is holding steadfast in Apple Pay's security system, making this issue as something that must be addressed by the card-issuing banks, partly because banks are responsible for determining the authorization process for a card to be loaded onto Apple Pay.[209] Such authorization processes could entail, for example, verification through voice, via a telephone call, or by email.[210] Apple leaves this verification process to the banks because, at this point in time, if a stolen card is uploaded to Apple Pay and used for purchases, the bank or credit card company is liable for the charges because Apple is not subject to EFTA while the banks/credit card companies are.[211] Banks and credit card companies should push for Apple Pay to be subject to EFTA, GLBA, and BSA because it would alleviate some of the burden of both fraud liability and verification requirements from the banks and credit card companies by placing some of it on Apple.[212]

While it is incredibly difficult to make a quantitative comparison

---

205. Hayley Tsukayama & Sarah Halzack, *Apple Pay's Pitch: Simpler is Better. But Some Security Experts Disagree*, THE WASH. POST: TECH. (Mar. 23, 2015), http://www.washingtonpost.com/business/technology/apple-pays-pitch-simpler-is-better-but-some-security-experts-disagree/2015/03/23/4b22520c-cd7b-11e4-8c54-ffb5ba6f2f69_story.html.

206. Nicole Arce, *Thieves Using Stolen Credit Card Data on Apple Pay: Who's Responsible*, TECH TIMES, (March 6, 2015, 8:55 AM), http://www.techtimes.com/articles/37756/20150306/thieves-using-stolen-credit-card-data-on-apple-pay-whos-responsible.htm.

207. Jose Pagliery, *Apple and Banks Dismiss Apple Pay Fraud Worries*, CNN MONEY (Mar. 18, 2015, 10:08 AM), http://money.cnn.com/2015/03/18/technology/apple-pay-fraud/.

208. *Id.*

209. Olga Kharif, et. al., *Banks Changing Apple Pay Procedures after Fraud, Consultants Say*, BLOOMBERG BUS. (Mar. 5, 2015, 11:11 PM), http://www.bloomberg.com/news/articles/2015-03-06/banks-changing-apple-pay-procedures-after-fraud-consultants-say.

210. *Id.*

211. *Id.*; *see also*, *supra* Part IV(A).

212. Rubenfeld, *supra* note 10; *see also supra* Part IV.

of "security," if there is a breach that is obvious to spot, especially a preventable one, then it would make sense, both financially and ethically, for a company to strive to do everything it could, within the realm of financial feasibility, to prevent it.[213] The credit card industry switched from magnetic strip technology to "chip and PIN" after an obvious flaw was exposed.[214] Given that chip technology was a feasible solution to the obvious flaws of magnetic technology, the credit card industry should serve as an example of self-regulation.[215] Given the propensity of criminals to expose flaws in data security, such major industry players, like Apple, should not play chicken with its customers' livelihoods and should strive to make its products as secure as possible.

G. Effect of Heightened Regulation on Apple

If Apple is forced to set up an AML program, make certain disclosures to users, and file SARs, as required under BSA,[216] or create a written information security plan, as required under GLBA,[217] it will reduce the amount of fraudulent payments that banks and credit card companies will have to pay out.[218] Apple may argue that any security threat could be lessened by increased verification requirements by banks. However, the cost of implementing a verification program can burden small banks, which already face liability for any fraud that occurs through Apple Pay, whereas Apple can easily afford to develop a security plan that includes AML, SARs, and disclosures to users.[219] Furthermore, while Apple may pass the short-term costs of heightened security on to

213. *See* GEMALTO, THE MIGRATION TO EMV CHIP TECHNOLOGY, http://www.pymnts.com/assets/Shared/Gemalto-EMV-Whitepaper.pdf 1-3 (last visited Sep. 30, 2015) (explaining how the major credit card companies were the ones behind the shift to Chip and PIN technology in the U.S. and how they did not wait for politicians to force change).

214. *Id.* at 3.

215. *Id.*

216. Bank Secrecy Act, 31 U.S.C. § 5330 (2012), 31 C.F.R. § 1022.210(a) (2015).

217. The Gramm-Leach-Bliley Act, 15 U.S.C. § 6809 (2012), 16 C.F.R. § 313.4(a) (2015).

218. OFFICE OF THE COMPTROLLER OF THE CURRENCY, MONEY LAUNDERING: A BANKER'S GUIDE TO AVOIDING PROBLEMS 3 (2002), http://www.occ.gov/topics/bank-operations/financial-crime/money-laundering/money-laundering-2002.pdf.

219. *See* Press Release, Kristin Huguet, et. al., Press Contacts, Apple, Apple Reports Record Fourth Quarter Results (Oct. 27, 2015) (illustrating how Apple had a net profit of over $10 billion in recent quarters and could afford to pay to develop compliance programs).

the issuing banks and card companies, it will likely save the banks and credit card companies money in the long term by reducing the frequency and impact of fraud. There is an ever-present risk to the companies, including card issuers, banks, and merchants, that have agreements with Apple Pay that if Apple Pay continues unchecked by regulation and is a key player in the mobile wallet market, that it will increase its fees from 0.15% per transaction to much higher amounts, such as up to the 3% fee that some credit card companies currently charge.[220] While heightened regulation is unlikely to prevent Apple from raising fee amounts, it will ensure that banks, merchants, and card issuers are not paying heightened fees without adequate protection from Apple.

V. MOVING FORWARD FOR APPLE PAY

If Apple Pay is considered to be a money transmittal business, then it would be required to register with FinCEN as an MSB and would be forced to establish a written anti-money laundering program.[221] Furthermore, Apple would also be required to keep a record of the order of transmittal of funds[222] and be required to report suspicious activity.[223] Requiring Apple to establish an anti-money laundering program would not shift the burden of verification requirements from the banks to Apple, but would simply require Apple to take adequate precautions against fraud, which would likely include Apple initiating mandatory verification standards.[224] Additionally, extending EFTA Regulation E to explicitly include the platform utilized by Apple Pay would force Apple to disclose several things to users such as a telephone number and address where users could reach Apple, the confidentiality standard that Apple is held to, and receipts or periodic statements to the users of Apple Pay.[225] Lastly, and most importantly, amending GLBA to explicitly include all mobile payment platforms would force Apple to set up a written

220. WIGLEY + COMPANY SOLICITORS, *supra* note 94.

221. 31 C.F.R. § 1022.210(a).

222. *Id.* § 1010.410(e).

223. *Id.*

224. Bank Secrecy Act, 31 U.S.C. § 5330 (2012), 31 C.F.R. § 1022.210(d)(1)(i)(A) (2015).

225. Electronic Funds Transfer Act, 15 U.S.C. § 1693 (2012), Electronic Funds Transfer Regulation E, 12 C.F.R. § 1005.7(b) (2015).

information security plan to protect its user's valuable information.[226]

If Apple were to register with FinCEN and be regulated by EFTA, it would not immediately debilitate Apple and would benefit all involved parties.[227] The civil fine for failing to register with FinCEN is a $5,000 *per day* violation,[228] which can add up over time.[229] The real financial burden would come with having to establish a system of reporting suspicious activity.[230] Furthermore, Apple would have to take adequate measures against fraud and devote significant resources to establishing an anti-money laundering program.[231] These costs would probably be absorbed by Apple, but if Apple is aggressive, it could be passed on to the banks and credit card companies.[232] If Apple's market share continues to grow to a point where it eventually dominates the mobile payment industry, then it is likely that it will increase its fees from 0.15% per transaction, to a number which is closer to the 1.5% to 3.0% range charged by most current credit card companies per transaction,[233] making it all the more important for it to face regulation. The upfront costs of creating a plan, hiring a compliance officer, training employees, and conducting audits,[234] which are a relatively small cost to Apple and likely to be passed on to banks and credit card companies, would be more than made up for by Apple if, by being regulated, Apple gains the trust of its target market and increases its customer base.

Subjecting Apple Pay to federal regulation would benefit Apple, financial institutions, and users alike. Although there are distinct differences between Apple Pay and other forms of electronic/mobile

---

226. The Gramm-Leach-Bliley Act, 15 U.S.C. § 6809 (2012), 16 C.F.R. § 313.4(a) (2015).

227. *See* Press Release, *supra* note 219 (illustrating how Apple had a net profit of over $10 billion in recent quarters and could afford to pay a relatively small fine).

228. 31 U.S.C. § 5330(e)(1).

229. *Id.*

230. *The Global Cost of Anti-Money-Laundering Efforts*, PYMNTS, (Feb. 24, 2014, 6:14 AM), http://www.pymnts.com/news/2015/the-global-cost-of-anti-money-laundering-efforts/.

231. *Id.*

232. *See* Charles Cooper & Greg Sandoval, *Apple's Big Win Over Samsung – What Does It Mean?*, CNET (Aug. 24, 2012, 6:44 PM), http://www.cnet.com/news/apples-big-win-over-samsung-what-does-it-mean/ (illustrating how the tech industry is known to pass costs of judgments and other matters on to consumers).

233. *See* PYMNTS, *Apple Pay's Business Model Blues*, *supra* note 96 (explaining how U.S. markets are open to interchange fees already, and would be susceptible to higher fees).

234. *Anti-Money Laundering ("AML") Programs*, *supra* note 173.

payment that keep Apple Pay out of the reach of current regulation, Apple Pay poses a greater need for regulation than its competitors because of the ever-present and increasing security threat to the public along with Apple Pay's endorsement from the federal government.

MAXWELL L. GREGSON