What's in Your Mobile Wallet? An Analysis of Trends in Mobile Payments and Regulation

Carolyn Lowry *

TABLE OF CONTENTS

* J.D., The George Washington University Law School, May 2016. Notes Editor, Federal Communications Law Journal.

I. INTRODUCTION

In September 2014, Apple announced the launch of Apple Pay, a mobile payments solution integrated into the new generation of iPhones, joining Google Wallet as a mobile payments option.[1] A few months later, Microsoft began applying for state money transfer licenses, a move that all but confirms Microsoft's soon-to-occur entry into the mobile payments space.[2] These announcements are significant because mobile payments, while popular in other countries, have been generally slow to catch on in the United States.[3] The emergence of technologies and services like Square, Uber, and Apple Pay allows consumers to leave their checkbooks, cash, and even wallets at home, a shift that could significantly transform commerce and business.[4] In fact, the idea for Venmo, a mobile payment application (app), came about in 2009 when one of the cofounders forgot his wallet and wondered why he was not able to simply transfer money to his friend through his cell phone instead of dealing with cash or paper checks.[5] The shift from paper to plastic to digital for everyday activities and transactions may seem far off to some, but increased convenience, security protections, and endorsement and adoption by government entities and major retailers may make the shift to e-wallets and mobile payments a near-term reality.

Mobile payments emerged as the result of the colliding worlds of technology and banking. As these industries collaborate and merge together, financial regulations must be examined to ensure existing regulations are able to provide the appropriate protections to consumers and, if not, to determine how such regulations should be modified to meet our increasingly mobile-centric world. Historically, banking has been a very heavily regulated industry, with state-level agencies and several federal government

---

1. Press Release, Apple, Apple Announces Apple Pay (Sept. 9, 2014), http://www.apple.com/pr/library/2014/09/09Apple-Announces-Apple-Pay.html.

2. *See, e.g.*, Matt Krantz, *Apple Pay Faces Another Problem*, USA TODAY (Apr. 6, 2015, 1:37 PM), http://americasmarkets.usatoday.com/2015/04/06/apple-pay-has-another-problem/.

3. Laurence Witherington & Henry Williams, *Apple Pay Moves World Closer to Mobile Payment Acceptance*, WALL ST. J. (Oct. 31, 2014, 7:39 AM ET), http://online.wsj.com/articles/apple-pay-moves-world-closer-to-mobile-payment-acceptance-1414755547.

4. *See, e.g.*, Aaron Klein, *Pocket Policy: Do New Technologies Need New Rules?*, BIPARTISAN POL'Y CTR. (Dec. 17, 2014), http://bipartisanpolicy.org/blog/pocket-policy-do-new-payments-technologies-need-new-rules/. The Iowa Department of Transportation also considered the potential for wallet-less living and recently announced the development of a smartphone app that would contain a digitally-encoded drivers license that would replace the commonly-used plastic card. *See* Joyce Russell, *A Plan To Put Your Driver's License On Your Phone*, NPR: ALL TECH CONSIDERED (Jan. 7, 2015, 5:46 PM), http://www.npr.org/blogs/alltechconsidered/2015/01/07/375658605/a-plan-to-create-put-your-drivers-license-on-your-phone.

5. Felix Gillette, *Cash is for Losers!*, BLOOMBERG (Nov. 20, 2014, 6:32 AM EST), http://www.bloomberg.com/bw/articles/2014-11-20/mobile-payment-startup-venmo-is-killing-cash.

agencies overseeing the financial services space, including the Federal Reserve, Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), Securities and Exchange Commission (SEC), and the Commodity Futures Trading Commission (CFTC). Additionally, the financial crisis and resulting Dodd-Frank Act led to the establishment of the Consumer Financial Protection Bureau (CFPB), an entire agency devoted to consumer financial protection. There are also state-level banking agencies and regulators in addition to state attorneys general. Compared to the banking and financial services industry, the mobile industry experiences a fairly hands-off approach with respect to regulation, despite its predecessors in the wireline industry being heavily monitored.

As technology becomes more ingrained in our lifestyles, products are emerging that straddle the financial services and wireless industries. For example, mobile wallets such as Apple Pay and Google Wallet are both apps, which are functionally a feature of a phone, not a new financial service or provider. Regardless of this distinction, because of the association of mobile payments with financial services, the legacy baggage of regulation exists.

As use of technology grows and the adoption of mobile payments becomes more prevalent, regulators will likely increase their level of attention and scrutiny upon these products. These new mobile payment technologies have raised the question of whether existing regulations are sufficient and provide an appropriate level of protection to consumers. The legal and regulatory framework affecting mobile payments should be comprehensive and effective while at the same time allowing innovation and development of new products. While existing regulations relating to payments were drafted before the emergence of mobile payments, these existing regulations provide robust legal protections for consumers. The introduction of new technology does not render existing regulations inapplicable, and point-of-sale mobile payments should legally be treated the same as the traditional, underlying transactions. Creating an additional layer of regulations could cramp innovation and lead to consumer confusion.

Part II of this Note provides an overview of the development of mobile payments, the types of mobile payments, and existing regulations that apply to electronic and mobile payments. Part III critically analyzes the extent to which existing legal and regulatory frameworks apply to mobile payments and examines the transformative effect that mobile payments may have on commerce. Part IV concludes that existing regulations are sufficient to protect consumers while allowing for innovation.

II. BACKGROUND

A. Mobile Has the Potential to Significantly Change Commerce and Business.

Mobile phones have revolutionized the way that people interact, communicate, shop, and conduct business. It is estimated that 2.6 billion people worldwide use smartphone mobile devices that are Internet-enabled, with this number predicted to more than double to 6.1 billion by 2020.[6] In the United States, use of mobile phones is similarly widespread, as shown by 87 percent of the U.S. adult population owning a mobile phone and 71 percent of these mobile phones being smartphones.[7] The availability of Internet on-the-go is changing the way that people shop and conduct financial business, and the mobile payments industry is expected to grow and become mainstream.[8] Recent studies have reflected this predicted growth; 17 percent of mobile phone users made a mobile payment in 2013, increasing to 22 percent in 2014.[9] This growth is expected to be "explosive" over the next few years, with a Business Insider Intelligence report predicting growth of the U.S. mobile payment volume at a five-year compound annual growth rate of 172 percent, increasing from less than $100 billion in 2014 to more than $800 billion in 2019.[10]

It is interesting to note, however, that the prevalence of mobile phone use for commerce and banking varies significantly by country and for a variety of reasons.[11] While some countries are still tied to the brick-and-mortar bank, others have adopted newer mobile-based technologies such as mobile payments through text-based data transfers.[12] Many of these technologies have been widely adopted, as illustrated by the fact that in nine

---

6. Ingrid Lungen, *6.1B Smartphone Users Globally by 2020, Overtaking Basic Fixed Phone Subscriptions*, TECHCRUNCH (June 2, 2015), http://techcrunch.com/2015/06/02/6-1b-smartphone-users-globally-by-2020-overtaking-basic-fixed-phone-subscriptions/.

7. BD. OF GOVERNORS OF THE FED. RESERVE SYS., CONSUMER AND MOBILE FINANCIAL SERVICES 2015, at 1 (2015), http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201503.pdf.

8. *See* Jason Ankey, *Financial Execs Survey: Mobile Payments Going Mainstream by 2015*, FIERCEMOBILECONTENT.COM (July 13, 2011), http://www.fiercemobileit.com/story/financial-execs-survey-mobile-payments-going-mainstream-2015/2011-07-13 (finding that 83 percent of financial services, technology, telecommunications, and retail executives expect mobile payments will achieve widespread mainstream consumer adoption by 2015).

9. BD. OF GOVERNORS OF THE FED. RESERVE SYS., *supra* note 7, at 1.

10. John Heggestuen, *The Apple Pay Effect Is Real — In-Store Mobile Payments Volume Will Top $800 billion in 2019*, S.F. CHRON. (Mar. 20, 2015, 6:02 AM), http://www.sfgate.com/technology/businessinsider/article/Mobile-Payments-Are-Poised-To-Explode-This-Year-4526391.php (forecasting that by 2019, 15 percent of all payment volume will occur through mobile devices).

11. *See id.*

12. Leo Mirani, *How to Manage All Your Financial Affairs from a $20 Mobile Phone*, QUARTZ (June 19, 2014), http://qz.com/218988/how-to-manage-all-your-financial-affairs-from-a-20-mobile-phone/.

African countries, the number of mobile money accounts exceeds the number of traditional bank accounts, providing a payment solution for many who may otherwise be unbanked or underbanked.[13] This widespread adoption of mobile payments in Africa has not gone unnoticed; both government and business have realized this trend and found ways to make use of mobile payments.[14]

Nordic countries have similarly experienced a shift towards cashless societies.[15] Denmark has taken great strides toward adopting mobile payments, with 1.8 million of the country's 5.6 million residents using an app provided by Danske Bank called "MobilePay."[16] The Danish government has even gone as far as proposing regulations that would make retail businesses no longer required to accept cash payments, with the goal of economic growth through reduced costs and increased productivity.[17]

While mobile payments have been successful in some global markets, they have been slower to catch on in the United States.[18] One major reason for this is that the United States has a robust banking system that promotes traditional financial products like credit cards and debit cards. While it cannot be overlooked that approximately one out of every four Americans is "unbanked"[19] or "underbanked,"[20] more than three out of four African adults

13. *Id.* The nine countries are Cameroon, the Democratic Republic of the Congo, Gabon, Kenya, Madagascar, Tanzania, Uganda, Zambia, and Zimbabwe.

14. *See, e.g.*, *Tanzania Collects Billions in Mobile Money Tax*, IT NEWS AFRICA (Sept. 9, 2013), http://www.itnewsafrica.com/2013/09/tanzania-collects-billions-in-mobile-money-tax/ (stating that the Tanzania Revenue Authority reported success with accepting mobile payments for tax bills and annual motor vehicle licensing fees); *see also* Jake Kendall et al., *Sub-Saharan Africa: A Major Potential Revenue Opportunity for Digital Payments*, MCKINSEY & CO. INSIGHTS & PUBL'NS (Feb. 2014), http://www.mckinsey.com/insights/financial_services/sub_saharan_africa_a_major_potential_revenue_opportunity_for_digital_payments (finding Sub-Saharan Africa an attractive market for mobile financial services growth and investment).

15. *Nordic Countries Point Way to Cashless Future as U.S. Struggles with Chip-and-Pin*, GUARDIAN (Jan. 9, 2015, 11:25 AM EST), http://www.theguardian.com/money/2015/jan/09/nordic-countries-cashless-societies-us-chip-pin; *see also* Liz Alderman, *Going Cashless in Sweden*, N.Y. TIMES (Dec. 26, 2015), http://www.nytimes.com/2015/12/27/business/international/in-sweden-a-cash-free-future-nears.html (remarking that in Sweden, cash accounts for only 20% of consumer transactions, compared to 75% in the rest of the world).

16. *Id.*

17. Doug Bolton, *Denmark Moves Closer to a Cashless Society*, INDEPENDENT (May 7, 2015), http://www.independent.co.uk/news/world/europe/denmark-moves-closer-to-a-cashless-society-10231995.html.

18. *See* Mirani, *supra* note 12; *see also* FED. DEPOSIT INS. CORP., 2013 FDIC NATIONAL SURVEY OF UNBANKED AND UNDERBANKED HOUSEHOLDS: EXECUTIVE SUMMARY 3 (Oct. 2014) [hereinafter *FDIC Survey*], https://www.fdic.gov/householdsurvey/2013execsumm.pdf.

19. The FDIC defines "unbanked" as households that do not have an account at an insured financial institution. *FDIC Survey*, *supra* note 18, at 3.

20. The FDIC defines "underbanked" as households that households that have an account, but have also obtained financial services and products from nonbank, alternative financial services providers in the prior 12 months. *Id.*

lack a bank account or financial product with a formal banking entity.[21] As a result, mobile payments have been an attractive option for many people in Africa who do not have access to traditional banking products, whereas a widely used banking and payment system has contributed to the slower adoption of mobile payments in the United States.[22] Even with a widely used and robust payment system, however, approximately 88 million Americans are unbanked or underbanked and lack access to bank accounts and credit scores,[23] which means that they lack access to the mainstream financial system that is so important to paying bills, building credit, buying a home, and sending a child to college. These unbanked and underbanked consumers often turn to alternative financial services providers, like payday lenders or check-cashing locations, in order to cash checks and make ends meet.[24] Payday lenders are often unregulated and charge higher fees,[25] a practice that has drawn the attention of the CFPB.[26]

Growth in the mobile payments industry may provide opportunities to shift unbanked and underbanked consumers toward more affordable and more regulated banking and financial products and services. Consider, for example, the efficiencies, increased convenience, and potential innovation that could occur with mobile payments by aligning the 1.3 billion active credit and debit cards with the nearly 7.3 billion active mobile phone accounts, two billion of which are smartphones.[27]

B. Mobile Devices Can Be Used to Make Various Types of Payments.

In the United States, there are five methods for processing payment transactions: cash, checks, credit and debit card rails, automated clearing

21. *See* Aaron Oliver, *Unbanked in Africa See Inclusion through Mobile Financial Services*, MASTERCARD (Mar. 19, 2014), https://newsroom.mastercard.com/2014/03/19/unbanked-in-africa-see-inclusion-through-mobile-financial-services/.

22. *See* Mirani, *supra* note 12.

23. Gosia Glinska, *Fighting Financial Exclusion: How to Serve 88 Million Americans Who Have No Bank*, FORBES (June 5, 2014, 11:48 AM), http://www.forbes.com/sites/darden/2014/06/05/fighting-financial-exclusion-how-to-serve-88-million-americans-who-have-no-bank/.

24. *Id.*

25. *See* Niraj Chokshi, *Payday Loans Suck Up Billions in Fees in States Where They're Unregulated*, WASH. POST (Sept. 11, 2013), http://www.washingtonpost.com/blogs/govbeat/wp/2013/09/11/payday-loans-still-suck-up-billions-in-fees-in-states-where-theyre-unregulated/.

26. *See* Press Release, Consumer Fin. Prot. Bureau, CFPB Considers Proposal to End Payday Debt Traps (Mar. 26, 2015), http://www.consumerfinance.gov/newsroom/cfpb-considers-proposal-to-end-payday-debt-traps/.

27. *The Mobile Pay Revolution*, MORGAN STANLEY BLUE PAPERS (Jan. 23, 2015), http://www.morganstanley.com/ideas/mobile-pay-taps-global-growth/.

house (ACH) rails, and wire transfers.[28] Payments can take place in person or electronically, and the emergence of new technologies and devices has shifted how consumers conduct their banking and purchasing. The connectivity and power of a mobile phone has potential to develop products and applications that provide better services at a lower cost.[29]

The term "mobile payments" can refer to a variety of transactions, and most consumers use a credit or debit card for the underlying payment transaction. Mobile payments can be made through the web browser of a mobile device, through text message, via a mobile application, or through a point-of-sale or Near Field Communication transaction.

1. Mobile Payments Can Be Made Through Websites or Mobile Apps, Facilitating Remote Transactions

Many may think that mobile payments in their most basic form are payments made through web browsers, such as purchases through retailers' traditional websites. For example, a consumer who is on-the-go but needs to purchase something online, such as a train ticket or a birthday gift for mom, can use a mobile device to access websites like amtrak.com or macys.com. These mobile transactions occur through the company's existing website and are treated the same as transactions made through the browser on a desktop or laptop computer.

Realizing that mobile phones provide new opportunities for consumer engagement, many companies involved in e-commerce have developed mobile-friendly websites and stand-alone apps. Online commerce channels have grown four times faster at a global level than brick-and-mortar stores,[30] and these online payments have the potential to make purchases and transactions more convenient and user-friendly for customers. For example, the Amtrak app offers both purchase options and other features that are intended to increase convenience, such as the Amtrak rewards program, eTickets, and calendars.[31] Use of retail websites, however, remains much more prevalent than use of apps, which is a behavior that can be attributed to discovery and web searches.[32] Many people use search engines like

28. Erin F. Fonté, *Mobile Payments in the United States: How Disintermediation May Affect Delivery of Payment Functions, Financial Inclusion and Anti-Money Laundering Issues*, 8 WASH. J.L. TECH & ARTS 419, 422-23 (2013).

29. *The Future of Money: Hearing Before the H. Subcomm. on Fin. Inst. & Consumer Credit of the H. Comm. on Fin. Servs.*, 112th Cong. (2012) (statement of Marla Blow, Assistant Dir., Card and Payment Markets, Consumer Financial Protection Bureau), http://financialservices.house.gov/UploadedFiles/112-142.pdf.

30. *The Mobile Pay Revolution*, *supra* note 27.

31. *See Amtrak app*, APPLE ITUNES PREVIEW, https://itunes.apple.com/us/app/amtrak/id405074003 (last accessed Mar. 14, 2015).

32. *See Mobile Web Outpaces Apps for Retail Transactions*, EMARKETER (Mar. 4, 2015), http://www.emarketer.com/Article/Mobile-Web-Outpaces-Apps-Retail-Transactions/1012138.

Google to locate an online retailer or product, and the search results tend to be more likely to lead the customer to a company's website rather than an app.[33]

Banks have also developed apps that strive to allow consumers to conduct banking both conveniently and securely.[34] Mobile banking is generally linked to traditional banking products like checking accounts, savings accounts, and credit cards.[35] Adoption of mobile banking has been fairly successful, with over fifty percent of smartphone owners using their smartphone devices to access mobile banking, whether it be to check account balances, transfer money between accounts, deposit checks, or other banking activities.[36] Consumers may also use their mobile banking applications to pay bills and, in the United States, the most basic and common form of mobile payment was the payment of a bill through an online system.[37] All major U.S. banks offer bill pay services through mobile payments.[38]

Mobile payments can also be conducted through websites and applications specifically designed to transfer money, as opposed to traditional brick-and-mortar banks that use online banking to supplement their existing business. Examples of these web-based payment providers are PayPal and Venmo, which allow consumers to transfer money to customers or "friends."[39] These providers generally need to acquire a money transmitter license from state regulators in order to do business.[40]

33. *Id.*

34. BD. OF GOVERNORS OF THE FED. RESERVE SYS., *supra* note 7, at 1.

35. *See Consumers and Mobile Financial Services March 2012: Current Use of Mobile Banking and Payments*, BD. OF GOVERNORS OF THE FED. RESERVE SYS., https://www.federalreserve.gov/econresdata/mobile-devices/2012-current-use-mobile-banking-payments.htm (last visited June 17, 2016) (defining mobile banking as "using a mobile phone to access your bank account, credit card account, or other financial account. Mobile banking can be done either by accessing your bank's web page through the web browser on your mobile phone, via text messaging, or by using an application downloaded to your mobile phone").

36. BD. OF GOVERNORS OF THE FED. RESERVE SYS., *supra* note 7, at 1.

37. *Id.*

38. DIV. OF DEPOSITOR & CONSUMER PROT., FED. DEPOSIT INS. CORP., ASSESSING THE ECONOMIC INCLUSION POTENTIAL OF MOBILE FINANCIAL SERVICES 25 (2014) (citing JAVELIN STRATEGY & RESEARCH, 2013 MOBILE BANKING FINANCIAL INSTITUTION SCORECARD (2013)), https://www.fdic.gov/consumers/community/mobile/Mobile-Financial-Services.pdf.

39. Sharon Profis, *Five Ways to Get People to Pay You Back (Compared)*, CNET (Feb. 10, 2015, 3:00 AM PDT), http://www.cnet.com/how-to/square-vs-venmo-vs-google-wallet-vs-paypal/.

40. For an overview of state money transmitter registration requirements, *see* THOMAS BROWN, 50-STATE SURVEY: MONEY TRANSMITTER LICENSING REQUIREMENTS, http://abnk.assembly.ca.gov/sites/abnk.assembly.ca.gov/files/50%20State%20Survey%20-%20MTL%20Licensing%20Requirements(72986803_4).pdf (last visited June 17, 2016).

2. Mobile Payments Can Be Made Through Text Message Transactions

Another type of mobile payment is conducted through the use of short messaging service (SMS), a form of mobile phone texting.[41] Consumers with text messaging-enabled phones can send payments to merchants or other persons by sending text messages with details on payee and payment amounts.[42] Text message payments and remittances are particularly popular in countries with large populations of unbanked individuals or where the use of cash may be prevalent yet risky.[43] However, in the United States, SMS payments for specific causes, such as political contributions or contributions to certain Red Cross' initiatives have been somewhat successful, whereas use of SMS payments for everyday transactions has been slow to catch on.[44] Consumer protection issues also exist with SMS payments that are billed directly to mobile phone bills. This billing practice has led to "cramming," the fraudulent practice of adding unauthorized third-party charges to a customer's phone bill.[45] As a result of this cramming fraud, and associated enforcement actions taken by the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC), major wireless carriers in the United States have generally ended the practice of allowing third-party premium SMS charges.[46]

---

41. *See SMS*, NEW OXFORD AM. DICTIONARY (3d ed. 2010).

42. Meena Aharam Rajan, *The Future of Wallets: A Look at the Privacy Implications of Mobile Payments*, 20 COMMLAW CONSPECTUS 445, 447 (2012).

43. *See* Fonté, *supra* note 28, at 445-46.

44. While the United States has a well-established payments system compared to other countries, this may have in fact hampered development of mobile payments technologies. *See* Fonté, *supra* note 28, at 446. *But see, e.g.*, Steve Lackmeyer, *Oklahoma Tornadoes: Red Cross Agrees to Dedicate Text Donations to State Storm Relief Efforts*, NEWSOK (May 23, 2013), http://newsok.com/oklahoma-tornadoes-red-cross-agrees-to-dedicate-text-donations-to-state-storm-relief-efforts/article/3833632 (estimating that the Red Cross raised $3.8 million for Oklahoma tornado disaster victims through text message contributions)*;* Janie Lorber, *Obama's Campaign Quick to Capitalize on Text-to-Donate Option*, ROLL CALL (Oct. 24, 2012, 10:33 AM), http://www.rollcall.com/news/Obama-Campaign-Quick-to-Capitalize-on-Text-to-Donate-Option-218432-1.html (estimating that the Obama campaign raised $836,550 through text message donations).

45. *See* FED. COMM. COMM'N, FCC CONSUMER GUIDE: CRAMMING – UNAUTHORIZED CHARGES ON YOUR PHONE BILL (last reviewed June 10, 2016), http://transition.fcc.gov/cgb/consumerfacts/cramming.pdf.

46. *See* Press Release, Fed. Comm. Comm'n, AT&T Mobility to Pay $105 Million to Settle Wireless Cramming and Truth-in-Billing Investigation (Oct. 8, 2014), http://www.fcc.gov/document/att-pay-105-million-resolve-wireless-cramming-investigation-0; *see also* Lydia Beyoud, *T-Mobile, FTC May Be Close to Settlement on Cramming Charges*, BLOOMBERG BNA (Oct. 22, 2014), http://www.bna.com/tmobile-ftc-may-n17179906182/ (highlighting that in November 2013, T-Mobile, AT&T, Sprint, and Verizon said they planned to stop all billing for premium text services except charitable giving and political giving).

3. Mobile Payments Can Be Made Through Point-of-Sale Transactions

The likely area of growth in the mobile payments space, and primary focus of this paper, is point-of-sale (POS) transactions using smartphones, a type of proximity payment.[47] While a smaller group of consumers use their smartphones to make point-of-sale payments, it appears likely that this will be the growing segment of the mobile payments space in the United States.[48] Of this group, thirty-nine percent made the point-of-sale payment by scanning a barcode or Quick Response code[49] (QR code) available on the screen of the phone.[50] The standalone Starbucks app and the LevelUp app, both use QR codes to effectuate point-of-sale payments.[51] In each app, customers hold the mobile device in front of a countertop scanner and scan a user-specific on-screen barcode to remit payment.[52] Apps can also provide a tipping feature[53] and the Starbucks app is closely integrated with the My Starbucks Rewards loyalty program—attracting customers who appreciate the convenience of the app and the opportunity to earn rewards like free coffee.[54]

---

47. Cadie Thompson, *Near Field Communication the Next Mobile Boost?*, USA TODAY (Jan. 8, 2012, 2:24 AM), http://usatoday30.usatoday.com/tech/news/story/2012-01-08/cnbc-near-field-communication-mobile/52443756/1.

48. *See* BD. OF GOVERNORS OF THE FED. RESERVE SYS., *supra* note 7, at 1.

49. A Quick Response Code (QR Code) is a type of two-dimensional matrix barcode developed by the Japanese automobile industry in the 1990s. QR Codes can hold 100 times the amount of information compared to a traditional one-dimensional barcode and have consequently expanded beyond the auto industry into more mainstream logistics and advertising. *See* Andrew Tarantola, *How QR Codes Work and Why They Suck So Hard*, GIZMODO (Dec. 18, 2012, 2:20 PM), http://gizmodo.com/5969312/how-qr-codes-work-and-why-they-suck-so-hard.

50. *See* BD. OF GOVERNORS OF THE FED. RESERVE SYS., *supra* note 7.

51. *See* STARBUCKS, STARBUCKS MOBILE APPS AND PAYMENTS FACT SHEET (Mar. 2014), https://news.starbucks.com/uploads/documents/Fact_Sheet_-_Starbucks_Mobile_Apps_and_Mobile_Payment_-_MAR2014.pdf; *see also* Alyson Shontell, *Payment Startup LevelUp Thinks It Has Found a Way to Charge Merchants a 0% Credit Card Processing Fee*, BUS. INSIDER (Apr. 16, 2014, 10:03 AM), http://www.businessinsider.com/levelups-cheap-credit-card-processing-fee-heading-towards-0-2014-4.

52. Lauren Johnson, *Starbucks Looks to Share Its App Payment System with Other Retailers*, ADWEEK (July 25, 2014, 9:54 AM), http://www.adweek.com/news/technology/starbucks-looks-share-its-app-payment-system-other-retailers-159100.

53. *See, e.g.*, *Starbucks app*, APPLE ITUNES PREVIEW, https://itunes.apple.com/us/app/starbucks/id331177714?mt=8 (last accessed Mar. 2, 2016); *LevelUp app*, APPLE ITUNES PREVIEW, https://itunes.apple.com/us/app/levelup-.-pay-with-your-phone/id424121785?mt=8 (last accessed Mar. 2, 2016).

54. *See* Dave Fortney, *Mobile Payments: Ready for Primetime*, 2 BANKING PERSPECTIVE, no. 3, 2014, https://www.theclearinghouse.org/publications/2014/banking-perspective-q32014/mobile-payments-ready-for-primetime.

Mobile payments also benefit small businesses and entrepreneurs.[55] For instance, payee-side mobile payment applications loaded on a business's smartphone or tablet allowing electronic payments with a small device like Square, as opposed to a more traditional credit or debit card processing machine.[56] Square services are available worldwide and allow small businesses to use specialized software on a phone or tablet to accept card payments.[57] Alternatively, the payer-side LevelUp app, which allows customers to pay any participating merchant via a credit or debit-linked QR code,[58] charges lower transaction fees than other credit card processors, purportedly making it more affordable for merchants than Square or MasterCard.[59] LevelUp allows businesses that cannot afford their own branded app to seize upon the efficiencies mobile payments generate.

An increase in point-of-service mobile payments is also expected to occur with Near Field Communication (NFC),[60] the "tap-and-go" technology used by mobile wallets such as Google Wallet, SoftWallet (formerly known as Isis[61]), and Apple Pay.[62] Mobile devices with NFC capabilities include a controller chip that is used for wireless communications between the POS terminal and the mobile device.[63] A consumer can make a purchase by positioning his or her phone near the NFC-enabled POS receiver.[64] A more detailed description of the technology

---

55. *See* Press Release, Fed. Comm. Comm'n, *supra* note 46, *see also* Beyoud, *supra* note 46.

56. *See The Mobile Pay Revolution*, *supra* note 27.

57. Richard Trenholm, *Square Register App Now Available to Small Businesses Around the World*, CNET (Nov. 20, 2014, 9:50 AM PST), http://www.cnet.com/news/square-register-app-now-available-to-small-businesses-around-the-world/.

58. *See* Shontell, *supra* note 51.

59. *See id.* (noting that LevelUp is both a mobile payment and advertising mechanism, which allows it to be one of the cheapest credit card payment processing option available to merchants).

60. *See* Fortney, *supra* note 54; *see also* Preeta M. Banerjee & Craig Wigginton, *Smart Device, Smart Pay*, DELOITTE UNIV. PRESS (June 23, 2015), http://dupress.com/articles/mpayments-mobile-pos-system-in-retail/ (predicting that 60 percent of smartphones will have Near Field Communication (NFC) capabilities by 2018).

61. *See* Jacob Kastrenakes, *ISIS Mobile Wallet Changes Name to Softcard to Avoid Association with Militant Group*, THE VERGE (Sep. 3, 2014, 8:40 AM), http://www.theverge.com/2014/9/3/6101035/isis-rebrands-as-softcard-to-avoid-association-with-militant-group.

62. *See* Witherington & Williams, *supra* note 3; *see also* Sarah Nassauer, *Retailers to Begin Public Tests of MCX Mobile Payment App But Face Hurdles*, *Wall St. J* (Aug. 11, 2015, 6:30 PM ET), http://www.wsj.com/articles/mcx-to-begin-public-tests-of-mobile-payment-app-but-faces-hurdles-1439332228 (noting that Merchant Customer Exchange (MCE), a consortium of retailers, launched a mobile wallet app in late 2015 known as CurrentC as a competitor to ApplePay); Mike Isaac, *Apple Pay Rival MCX Open to Other Technology*, N.Y. TIMES (Oct. 29, 2014), http://www.nytimes.com/2014/10/30/technology/rival-says-it-may-adopt-apple-pays-system.html.

63. *See* Sam Gustin, *Near Communications Big (Money) Moment*, WIRED (May 25, 2011, 3:59 PM), http://www.wired.com/picenter/2011/05/wired-nfc.faq/.

64. *See* Fonté, *supra* note 28, at 428.

is as follows: "Near Field Communication technology is a short-range tool that operates on wireless frequencies . . . . It works by connecting a user's mobile device, equipped with an NFC antenna . . . to a receiver, usually a few feet away.[65]

NFC technologies and devices have caught on more quickly than expected, with NFC-compatible terminals available at more than two million stores.[66] Analysts predict that 148 million consumers worldwide will make a contactless payment in 2016.[67] This growth is largely spurred by the adoption of Apple Pay, signing up 12 million users monthly since its launch in October 2014, and Android Pay, which has signed up 5 million users a month since September 2015.[68]

C. Payments Are Subject to a Variety of Existing Regulations

As new technologies develop in the payment space, regulators must ensure that appropriate protections are in place to safeguard consumers from fraud and unauthorized transactions.[69] Furthermore, companies should be encouraged to develop technologies that include sufficient privacy and security protections to reduce the chances of data breaches and associated fallout.[70] Particularly given the recent data breaches at retailers such as Target[71] and Anthem,[72] which affected tens of millions of consumers, it is essential that consumers can feel comfortable using their financial products, especially when new technologies are involved.[73]

---

65. Gustin, *supra* note 63.

66. Hilary Brueck, *Apple Pay is Going Somewhere New This Year*, FORTUNE (Mar. 24, 2016, 9:18 AM EDT), http://fortune.com/2016/03/24/apple-pay-gets-easier-to-use-this-year/.

67. Andrew Meola, *Apple Pay and Samsung Pay Continue to Dominate the Mobile Wallet Market*, BUS. INSIDER (Mar. 4, 2016, 10:38 AM), http://www.businessinsider.com/apple-pay-samsung-pay-lead-mobile-wallet-growth-2016-3.

68. Olga Kharif, *Samsung Gunning for Apple in Race to Dominate Mobile Payments*, BLOOMBERG TECH. (Mar. 1, 2016, 5:00 AM EST), http://www.bloomberg.com/news/articles/2016-03-01/samsung-gunning-for-apple-in-race-to-dominate-mobile-payments.

69. *See* Press Release, Consumer Fin. Prot. Bureau, CFPB Launches Inquiry into Mobile Financial Services (June 11, 2014), http://www.consumerfinance.gov/about-us/newsroom/cfpb-launches-inquiry-into-mobile-financial-services/.

70. *See* Press Release, Fed. Trade Comm'n, Staff Report on Mobile Shopping Apps (Aug. 1, 2014), https://www.ftc.gov/news-events/press-releases/2014/08/staff-report-mobile-shopping-apps-found-disclosures-consumers-are.

71. *See* Rachel Abrams, *Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop*, N.Y. TIMES (Aug. 5, 2014), http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html (explaining that December 2013 hack of Target's computer system compromised personal data and credit card information of twelve million customers, imposing significant costs on Target and hurting its stock price).

72. *See* Dan Munro, *Health Data Breach At Anthem Is A Blockbuster That Could Affect 80 Million*, FORBES: PHARMA & HEALTHCARE (Feb. 5, 2015, 9:36 AM), http://www.forbes.com/sites/danmunro/2015/02/05/health-data-breach-at-anthem-is-a-blockbuster-could-affect-80-million/ (explaining that Anthem experienced a data breach affecting the records of approximately 80 million customers).

73. *See* Press Release, Consumer Fin. Prot. Bureau, *supra* note 69.

Regulations currently exist that provide protections to purchases made by credit card and debit card, as well as stored-value cards such as prepaid or gift cards. Even though these forms of payment are generally used in the same manner, such as through a swipe at a grocery store or by entering the card information on a website, it is important to note that the regulations differ for each form of payment and, as a result, may have different consequences for consumers.

1. The Fair Credit Billing Act and Truth in Lending Act Protect Consumers' Credit Card Purchases

Fraudulent credit card transactions are protected under the Truth in Lending Act of 1968 (TILA)[74] and subsequent Fair Credit Billing Act of 1974 (FCBA).[75] Additionally, Regulation Z of the TILA provides protections to consumers using credit products, including credit cards.[76] Under Regulation Z, consumers are provided a means of fair and timely resolution of credit billing disputes.[77] Additionally, under the Fair Credit Billing Act (FCBA), a consumer's liability is limited to $50 for unauthorized or fraudulent charges.[78]

It is important to note that there are differences between protections for credit and debit cards. If there is a fraudulent charge involving a credit card, a customer's availability of credit is affected. This is different from a fraudulent charge on a debit card, which affects the availability of actual funds in a bank account. It is also important to consider that, with a credit card, a customer can withhold payment until the fraudulent charge is investigated.[79] Furthermore, many credit card issuers go beyond the statutory requirements of the FCBA and offer zero liability for customers who experience fraud.[80]

---

74. Truth in Lending Act, 15 U.S.C. §§ 1601-1667f (2012). TILA was originally adopted to prohibit unsolicited credit cards but has since been expanded to address a variety of consumer credit products. *See, e.g.*, CONSUMER FIN. PROT. BUREAU, CFPB CONSUMER LAWS AND REGULATIONS: TRUTH IN LENDING 1 (2013), http://files.consumerfinance.gov/f/201306_cfpb_laws-and-regulations_tila-combined-june-2013.pdf.

75. 15 U.S.C. § 1666 (2012).

76. 15 U.S.C. § 1601 (2012).

77. *See id.*

78. 15 U.S.C. § 1666; *see also Disputing Credit Card Charges*, FED. TRADE COMMISSION: CONSUMER INFO. (Aug. 2012), http://www.consumer.ftc.gov/articles/0219-disputing-credit-card-charges.

79. *Disputing Credit Card Charges*, *supra* note 78.

80. Allison Martin & Beverly Harzog, *Should Consumers Mostly Use Credit or Debit Cards?*, WALL ST. J. (Mar. 1, 2015, 11:37 PM), http://www.wsj.com/articles/should-consumers-mostly-use-credit-or-debit-cards-1425271054.

2. The Electronic Funds Transfer Act Protects Consumers Who Make Purchases by Debit Card

Fraudulent debit card transactions are protected under the Electronic Funds Transfer Act (EFTA), which is implemented by the Federal Reserve Board through Regulation E.[81] The EFTA outlines rights, responsibilities, and liabilities for consumers using electronic fund transfer (EFT) services.[82] A consumer's liability is dependent on the time period in which he or she reports a fraudulent charge to the card issuer.[83] If someone makes unauthorized transactions with a consumer's debit card number, the consumer has limited liability for those transactions if he or she reports them within 60 days of the statement being sent.[84] The EFTA also outlines the responsibilities and requirements of financial institutions offering EFT services.[85]

While there is limited liability for customers who use debit cards, it is important to note that there may still be drawbacks. For example, a customer who relies predominantly on a debit card and experiences a fraudulent purchase may experience cash flow issues.[86] The funds from the checking account that are used for the fraudulent transaction may be tied up while the bank or card issuer investigates and reimburses the unauthorized transaction.[87]

3. Purchases Made by Stored-Value Cards Are Provided Different Statutory Protections

Consumers can use stored-value cards like branded loyalty cards or "general purpose reloadable cards" (often called prepaid debit cards) to make mobile payments.[88] While historically less popular than debit or credit

81. 15 U.S.C. § 1693b, o-2 (2012); *see also* 12 C.F.R. § 205 (2015); *Disputing Credit Card Charges*, *supra* note 78. Regulation E covers any "transaction initiated through an electronic terminal, telephone, computer, or magnetic tape that instructs a financial institution either to credit or debit a consumer's account." Examples of EFT systems include "automated teller machine transfers, telephone bill-payment services, point-of-sale (POS) terminal transfers in stores, and preauthorized transfers from or to a consumer's account (such as direct deposit and social security payments)." BD. OF GOVERNORS OF THE FED. RESERVE SYS., REGULATIONS: COMPLIANCE GUIDE TO SMALL ENTITIES, http://www.federalreserve.gov/bankinforeg/regecg.htm (last visited on May 3, 2016).

82. 15 U.S.C. § 1693o-2.

83. *See id.*

84. 15 U.S.C. § 1693g.

85. 15 U.S.C. § 1693b.

86. *See* Martin & Harzog, *supra* note 80.

87. *See id.*

88. *See* John Adams, *Starbucks Mobile POS Success Shows Barcode's Potential*, AM. BANKER (Apr. 2011), http://www.americanbanker.com/bulletins/-1036436-1.html; *see also How Prepaid Cards Can Ignite Mobile Payments*, PYMNTS.COM (Dec. 16, 2013),

cards, use of prepaid cards has surged recently, with $37 billion loaded onto cards in 2010 and predictions of $80 billion or more by the end of 2014.[89] While this option may seem appealing and convenient for customers who want to control or limit the amount of their purchases or who want to reduce the risk of fraud by not using their primary credit card number, from a regulatory standpoint, this option is actually the least protected. Prepaid debit cards are not provided the same statutory protections as credit or debit cards, and only the FTC Act provides protections for unauthorized charges under existing federal law.[90] While the FDIC regulates accounts associated with credit and debit cards, the FDIC does not limit the liability for unauthorized use of most prepaid cards.[91] If an FDIC-member company issues a prepaid card, however, FDIC deposit insurance may kick in if the member company fails.[92]

The CFPB recently published proposed rules relating to general purpose reloadable cards in the fall of 2014, and these rules may have a substantial impact for consumers as well as companies looking to provide mobile payment options through these prepaid cards. The proposed rules would require companies issuing prepaid cards to provide increased consumer protections, including limitations on a consumer's losses when a card is lost or stolen.[93] Pending finalization of the CFPB's rules and with current regulatory protections for prepaid cards being fairly limited, some companies may fill in the statutory gaps through contractual provisions.[94] The FTC stresses that, while these protections are commendable, the protections are voluntary and can be withdrawn or modified at any time.[95]

---

http://www.pymnts.com/uncategorized/2013/how-prepaid-cards-can-ignite-mobile-payments/.

89. Carter Dougherty, *Fraud Protections for Prepaid Cards Proposed by Consumer Bureau*, BLOOMBERG (Nov. 13, 2014, 12:01 AM EST), http://www.bloomberg.com/news/articles/2014-11-13/fraud-protections-for-prepaid-cards-proposed-by-consumer-bureau.

90. *See* FED. TRADE COMM'N, REPORT: PAPER, PLASTIC . . . OR MOBILE? AN FTC WORKSHOP ON MOBILE PAYMENTS 6 (Mar. 2013), https://www.ftc.gov/sites/default/files/documents/reports/paper-plastic-or-mobile-ftc-workshop-mobile-payments/p0124908_mobile_payments_workshop_report_02-28-13.pdf.

91. *See* FED. DEPOSIT INS. CORP., TEN THINGS YOU SHOULD KNOW ABOUT DEBIT, CREDIT, OR PREPAID CARDS (Mar. 1, 2012), https://www.fdic.gov/consumers/consumer/information/ncpw/cardstopten.html.

92. *Id.*

93. *See* Press Release, Consumer Fin. Prot. Bureau, CFPB Proposes Strong Federal Protections for Prepaid Products (Nov. 13, 2014), http://www.consumerfinance.gov/newsroom/cfpb-proposes-strong-federal-protections-for-prepaid-products/.

94. *See* FED. TRADE COMM'N, *supra* note 90, at 7. (finding that some mobile payment providers that allowed funding from prepaid cards, voluntarily limited customer liability for fraudulent charges up to $50, similar to debit card protections).

95. *See id.*

4. Money Transfer Rules Vary by State and May Apply to Companies That Provide Certain Mobile Payment Transaction Services

Currently, all 50 states have money transmitter laws requiring licensure. The definition of "money transmission," however, varies by state. As a result, it can be challenging for money transmitter companies to develop and implement appropriate regulatory regimes that appropriate and sufficiently meet the requirements of the different jurisdiction.

One example of this is Square, a credit card and debit card payment system, which failed to register as a money transmitter and faced legal and enforcement actions in Florida and Illinois.[96] Regulations can differ depending on whether the transmitter accepts just credit and debit cards or whether the company accepts gift cards, as this activity involves "holding" rather than just "transferring" funds.[97] Companies offering mobile payment products and services should be aware of a state's definition of money transmitters and should register accordingly. Companies such as PayPal, Amazon, Facebook, and Google have taken a comprehensive approach to registration in response to pressure from a multistate alliance of regulators and have registered in all states with money transmitter laws.[98] Such an endeavor, however, can be incredibly time-consuming and can cost $500,000 or more for the required licenses.[99] These costs can be prohibitive and crippling, and in some states, such as California, the burden can be so high as to drive away business and stifle innovation.[100] These sorts of

96. *See, e.g.*, Ingrid Lunden, *Square Fined $507k in Florida for Operating a Mobile Payment Service Without a Money Transmitter License*, TECHCRUNCH (Aug. 16, 2013), http://techcrunch.com/2013/08/16/square-fined-507k-in-florida-for-operating-a-mobile-payment-service-without-a-money-transmitter-license/; Leena Rao, *Square Slapped With Cease And Desist By Illinois State Department Of Financial Regulation*, TECHCRUNCH (Mar. 1, 2013), http://techcrunch.com/2013/03/01/square-slapped-with-cease-and-desist-by-illinois-state-department-of-financial-regulation/. *See also* Sean Sposito, *Facebook Fast-Tracks Its Payments Business*, AM. BANKER (Feb. 21, 2012), http://www.americanbanker.com/issues/177_35/facebook-credits-money-transmitter-license-bank-regulation-1046825-1.html (noting that Facebook proactively sought money transfer licenses to avoid similar legal issues); *Money Transfer Licenses*, FACEBOOK, https://www.facebook.com/payments_terms/licenses (last visited June 18, 2016).

97. Tim Fernholz, *The Patchwork of Regulations Entangling Square, and Every American Internet Startup That Takes Money*, QUARTZ (Mar. 13, 2013), http://qz.com/62265/why-square-and-seven-other-finance-start-ups-got-run-out-of-illinois/.

98. *Id.*

99. *Id.*

100. *See* Owen Thomas, *This Innovation-Killing California Law Could Get a Host of Startups in Money Trouble*, BUS. INSIDER (July 11, 2012, 6:21 PM), http://www.businessinsider.com/california-money-transmitter-act-startups-2012-7 (arguing that California's money transfer law led FaceCash to withdraw from doing business in the state). FaceCash, now defunct, was an innovative payments start-up that created a mobile app that would enable participating merchants to view a photo of the consumer before approving a point-of-sale purchase. Fumiko Hayashi, *Mobile Payments: What's in It for Consumers?*

regulations, while purportedly put into place to protect consumers, are particularly burdensome for start-ups, thus inhibiting the development of innovative solutions and products.

5. Data Collected in Connection with Mobile Payments May Be Subject to Privacy and Data Security Regulations

Depending on the type of data transferred or stored and the user of the device, mobile payment providers may be subject to various privacy and data security regulations. As a result, companies should ensure that their products and services meet the requirements of these regulations in addition to the regulations that apply to financial transactions.

One of the significant risks for credit and debit cards is a data breach and the subsequent unauthorized use of personal and card data. Currently, there is no federal law that regulates data breaches, although some federal laws protect data in specific sectors like health and financial information.[101] Myriad state laws supplement these sector-specific federal laws, adding yet again to the patchwork of regulation. State law, as one might expect, is not uniform, and some states lack even basic privacy protections like data breach notification rules.[102] By September 2014, forty-seven states, the District of Columbia, the United States Virgin Islands, Guam, and Puerto Rico, have enacted data breach notification laws that require government and private entities to notify individuals of loss of personally identifiable information.[103] While the state regulations generally do not provide a private cause of action for individuals whose private information is breached,[104] the

---

ECON. REV. 1st Quarter 2012, at 35, 50, https://www.kansascityfed.org/publicat/econrev/pdf/12q1Hayashi.pdf.

The California money transmitter regulations, however, have since been amended. *See* Sean Sposito, *California Reforms Money Transmitter Law*, AM. BANKER (Oct. 13, 2013), http://www.americanbanker.com/issues/178_195/california-reforms-money-transmitter-law-1062691-1.html.

101. *See, e.g.*, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104–191, 110 Stat. 1936 (setting national standards for protection of electronic health care information); Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999) (setting national standards for protection of consumer information held by financial institutions); Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-6505 (2012) (giving FTC authority to regulate the collection and use of personal information from and about children under thirteen years old on the Internet).

102. *See* NAT'L CONFERENCE OF STATE LEGISLATURES, STATE SECURITY BREACH NOTIFICATION LAWS, (Sept. 4, 2014), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. As of the report's publication, only Alabama, New Mexico, and South Dakota do not have any data breach laws in place. *Id.*

103. *See id.*

104. Lance Bonner, *Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches*, 40 WASH. U. J.L. & POL'Y 257, 267 (2012).

compliance costs imposed on companies and governments can still be tremendously high.[105]

In conjunction with his 2015 State of the Union address, President Barack Obama introduced a package of cybersecurity and data security proposals, including the Personal Data Notification and Protection Act, which would establish a national standard for companies to notify employees and customers about security breaches, as well as a Consumer Privacy Bill of Rights.[106] Congress may choose to consider the President's proposals or other data protection and privacy bills during the 114th Congress, and such action could increase consumers' confidence with respect to their data transferred through electronic and mobile payments.[107]

D. The CFPB and FTC Have the Responsibility to Enforce Consumer Protection Laws

The FTC has broad jurisdiction in the commercial marketplace, and Section 5(a) of the Federal Trade Commission Act allows the FTC to take action against companies that engage in "unfair or deceptive acts or practices [UDAP] in or affecting commerce." [108] The FTC also has jurisdiction in certain circumstances over telecommunication providers, mobile phone operators, and nondepository providers of financial products or services.[109]

The CFPB has jurisdiction that is even broader than that of the FTC, although its application is limited to financial products and services. The Dodd-Frank Act builds off of the general consumer protection authority of the FTC Act and directs the CFPB to issue regulations and take action against companies engaging in "unfair, deceptive, and abusive acts or practices [UDAAP]" [110] This expands on the traditional consumer protection authority at the FTC, with the additional "A" standing for abusive, a term that at this time is fairly vague but is likely to be defined through the CFPB's rulemaking activities. Additionally, under the Dodd-Frank Act, the

105. *Id.* at 262.

106. Press Release, White House Office of the Press Sec'y, Fact Sheet: Safeguarding American Consumers & Families (Jan. 12, 2015), http://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families.

107. *See* AM. BANKERS ASS'N, THE CHANGING FACE OF THE PAYMENTS SYSTEM: A POLICYMAKER'S GUIDE TO IMPORTANT ISSUES 4 (2013), http://www.aba.com/Tools/Function/Payments/documents/2013EmergingPayments.pdf.

108. Federal Trade Commission Act §45(a), 15 U.S.C. §45(a)(2) (2012) (granting the FTC authority to prosecute unfair and deceptive trade practices, often referenced as UDAP, which was extended to banks under the Federal Deposit Insurance Act § 8, 12 U.S.C. § 1818 (2012), but is enforced by other agencies like the FDIC) *See* FED. DEPOSIT INS. CORP., FDIC COMPLIANCE EXAMINATION MANUAL – NOVEMBER 2015, at VII-1.1 (2015), https://www.fdic.gov/regulations/compliance/manual/ComplianceExaminationManual.pdf

109. *See* FED. TRADE COMM'N, *supra* note 90, at 3; *see also* 15 U.S.C. § 45(a)(2); 12 U.S.C. § 5581(b)(5)(c).

110. *See* Dodd-Frank Wall Street Reform and Consumer Protection Act §§ 1002, 1031, 1036(a), 12 U.S.C. §§ 5481, 5531 & 5536(a) (2012) (defining the provisions often referred to as UDAAP).

CFPB is granted jurisdiction over two entities: "covered persons" and "service providers."[111] The Dodd-Frank Act allows state attorneys general to bring civil actions against companies for violations of UDAAP.[112]

As will be further discussed below, companies involved with mobile payments may be covered by the CFPB's broad authority. The banks providing traditional financial products such as checking accounts, debit cards, and credit cards are clearly under the jurisdiction of the CFPB. What is important to note, however, is that the CFPB's UDAAP authority is not limited to financial services and could cover financial products, regardless of the provider or method of payment.[113]

III. IN ORDER FOR MOBILE PAYMENTS TO BE WIDELY ADOPTED, CONSUMERS NEED AN OVERWHELMING REASON TO CHANGE THEIR BEHAVIOR

The release of the iPhone in 2007, just a few short years ago, revolutionized the way that many consumers do business, communicate with friends and family, and get information. The growth of smartphones over the past few years has surpassed the growth of any other technology, including televisions and computers.[114] Mobile payments have also grown over the years, with 12 million users and 15 percent of United States revenue coming from mobile payments.[115] In order for mobile payments to become mainstream, however, consumers will need an overwhelming reason to change their behavior and will need to be assured that their mobile payment activity is secure, which may be a challenge in light of the recent card data breaches.[116]

One positive and potentially highly influential step in the direction of mainstream mobile payments was the announcement during a February 2015 White House Cybersecurity Summit that the federal government

111. 15 U.S.C. § 5481(6), (26) (2012) (defining the terms "covered person" and "service provider").

112. Dodd-Frank Wall Street Reform and Consumer Protection Act § 1042, 12 U.S.C. § 5552 (2012).

113. *See* Danielle Douglas-Gabriel, *Are Wal-Mart and Apple Poised to be Regulated by the CFPB?*, WASH. POST (Sept. 25, 2014), http://www.washingtonpost.com/news/business/wp/2014/09/25/are-wal-mart-and-apple-poised-to-be-regulated-by-the-cfpb/; *see also* Catherine Dunn, *Will Apple Pay Earn Oversight by the Consumer Financial Protection Bureau?*, INT'L BUS.TIMES (Sept. 12, 2014, 5:07 PM), http://www.ibtimes.com/will-apple-pay-earn-oversight-consumer-financial-protection-bureau-1687574.

114. *See* Fortney, *supra* note 54 (citing MARY MEEKER, KCPB INTERNET TRENDS 2014 95 (2014), http://www.kpcb.com/internet-trends).

115. *Id.*

116. *See* Richard Moulds, *Why Mobile Payment Adoption Has Been Slow – And Why That's About to Change,* WIRED (Jan. 2015), http://www.wired.com/2015/01/mobile-payments-adoption/.

would begin taking Apple Pay as payment in September 2015.[117] According to this announcement, Apple Pay will be accepted for admission fee payments at National Parks and will be linked to Social Security and veterans benefits.[118] The U.S. government is also expected to integrate Apple Pay into its GSA SmartCard programs for use with federal payment cards.[119] This announcement was viewed by many as a "vote of confidence" for the security of Apple Pay.[120] Developments like these in the payments space can be likened to an endorsement of the technology and are likely to have a positive effect on the growth and adoption of Apple Pay and similar mobile payment products.

The convenience factor of mobile payments should certainly not be overlooked or discounted. Mobile phones are compact and portable, and the integration of financial services into the device could eliminate the need to carry around a bulky wallet with multiple cards in addition to cash and coins.[121] Convenience with respect to time is also worth noting; some studies have estimated that transactions using contactless payment methods such as NFC can be 15 to 30 seconds faster than swiping a credit or debit card and signing or entering a PIN.[122] A study by Sweetgreen, a salad chain, found that using the LevelUp app to pay for purchases takes just seven seconds.[123]

A. Companies Involved with Mobile Payments Must Alleviate Consumers' Privacy and Fraud Concerns

In order for mobile payments to be widely adopted, consumers will need to be confident in the privacy and data security protections of mobile payment providers. While providers of mobile payments have touted security of this new technology, customers may remain skeptical until the technologies are tried and true. A Federal Reserve study found that concerns about the security of the technology were the primary reason given for not using mobile payments.[124] The adoption of Apple Pay by the federal government could be the stamp of approval needed to motivate and tip potential customers into integrating Apple Pay into their daily activities.

---

117. Press Release, White House Office of the Press Sec'y, Fact Sheet: White House Summit on Cybersecurity and Consumer Protection (Feb. 13, 2015), https://www.whitehouse.gov/the-press-office/2015/02/13/fact-sheet-white-house-summit-cybersecurity-and-consumer-protection; *see also* Michal Lev-Ram, *Tim Cook: Apple Pay Launching for Government Transactions*, FORTUNE (Feb. 13, 2015, 2:48 PM EDT), http://fortune.com/2015/02/13/tim-cook-apple-pay-government/.

118. Lev-Ram, *supra* note 117.

119. Andrea Peterson, *Apple Pay Gets a Big Vote of Confidence from the U.S. Government*, WASH. POST (Feb. 13, 2015), http://www.washingtonpost.com/blogs/the-switch/wp/2015/02/13/apple-pay-gets-a-big-vote-of-confidence-from-the-u-s-government/.

120. *Id.*

121. Hayashi, *supra* note 100, at 43.

122. *Id.* at 44.

123. Shontell, *supra* note 51.

124. BD. OF GOVERNORS OF THE FED. RESERVE SYS., *supra* note 7.

Consider, for example, that over 56 million Americans receive social security benefits.[125] Integrating Apple Pay into the daily use of even a fraction of these beneficiaries could drastically increase the number of users of Apple Pay.[126] As described in more detail below, mobile payment providers have taken key steps to ensure privacy, data security, and protection from fraud.

B. Businesses Should Strive to Ensure Mobile Payments Are Convenient for Customers

In order to facilitate widespread adoption of mobile apps by consumers, businesses will need to ensure that mobile payments are convenient for consumers. Businesses may need to utilize market research to determine how to maximize convenience. Starbucks, for example, enhanced its app with an option for customers to tip baristas through the app.[127] The development was thoughtful; customers may not find it convenient to pay for their drink through their phones, but at the same time, needing to dig into their wallet to find change to tip is anything but convenient.

Businesses may also want to consider integration with other apps and features to make sure that mobile payments are convenient as possible. Google, for example, has the potential to greatly influence a consumer through integration of payments space with other touch points like Google Maps, Gmail, etc.[128] The Motley Fool, a multimedia company providing financial advice, explains that the highly integrated environment for hypothetical Starbucks VIP customers provides the ultimate user experience:

> Straight from the app, you can order your black car service to pick you up and take you to your local Starbucks, where your drink is already waiting for you when you arrive since you've ordered and paid ahead of time through the app. It will also have your favorite daily newspaper loaded on your phone ready

125. SOC. SEC. ADMIN., SOCIAL SECURITY MONTHLY STATISTICAL SNAPSHOT: NOVEMBER 2015, at 1 (2015), https://www.ssa.gov/policy/docs/quickfacts/stat_snapshot/2015-11.pdf.

126. *Cf.* Kif Leswing, *Why It Matters that the Federal Government Will Accept Apple Pay*, GIGAOM (Feb. 13, 2015, 1:31 PM PDT), https://gigaom.com/2015/02/13/why-it-matters-that-the-federal-government-will-accept-apple-pay/.

127. Press Release, Starbucks, Digital Tipping and 'Shake to Pay' are New with Starbucks Enhanced App for iPhone (Mar. 11, 2014), http://news.starbucks.com/news/starbucks-accelerates-mobile-payment-leadership-with-release-of-enhanced-io. Starbucks states that the new app makes "the digital experience even easier and more rewarding for our customers and partners" and notes that, "As more and more customers are using their phone to pay, they have also asked for a convenient and meaningful way to show their appreciation to store partners." *Id.*

128. Mike Dautner, *Buy from the Map: Google Maps Advances into Mobile Payments*, PAYMENT WEEK (Nov. 16, 2015), http://paymentweek.com/2015-11-16-buy-from-the-map-google-maps-advances-into-mobile-payments-8860/.

> to read along with your coffee, and then have your private driver return you home, all without ever leaving the app.[129]

Companies can develop and implement different types of integrated experiences based on customer needs and demands.

C. Businesses May Need to Revamp or Incorporate New Incentives to Encourage Customers to Adopt Mobile Payments

Merchants and mobile payment providers should explore coupons and discounts for using mobile payments to incentivize the use of the mobile payment products. For example, the Starbucks app is considered highly successful, as shown by 10 million customers using the app for 5 million transactions each week.[130] Starbucks provides incentives for use of the app by offering app rewards such as free birthday drinks.[131] Businesses using the LevelUp app similarly reward loyal customers by providing free meals after multiple visits.[132]

Card issuers and businesses may also want to consider whether and how to incentivize customers to use mobile applications for payment. If mobile payments are, in fact, more secure than payments involving the traditional swipe of a credit or debit card, cost savings involved with issuing and processing cards could result.

IV. EXISTING LAWS AND REGULATIONS APPLY TO THE UNDERLYING TRANSACTIONS OF MOBILE PAYMENTS AND PROVIDE SUFFICIENT PROTECTIONS TO CONSUMERS

As described above, there is an existing framework of regulations that applies to payment transactions. This framework is robust and provides consumer protections against fraud across a variety of different financial products. These regulations are tied to the payment instrument (i.e., credit or debit card) and therefore provide the same protections, whether the instrument is used for an in-store, online, or mobile transaction. These existing regulations, coupled with the increased security measures put in place for mobile payment applications, should help lead to widespread adoption of mobile payments by consumers.

---

129. Seth McNew, *What Makes Starbucks' Mobile App Great?*, MOTLEY FOOL (Oct. 7, 2014, 6:22 PM), http://www.fool.com/investing/general/2014/10/07/what-makes-starbucks-mobile-app-great.aspx.

130. John Heggestuen, *Starbucks Generated Over $1 Billion From Mobile Transactions Last Year*, BUS. INSIDER (Jan. 31, 2014, 2:30 PM), http://www.businessinsider.com/mobile-payments-at-starbucks-explode-in-2013-passing-the-1-billion-mark-2-2014-1.

131. *Id.*

132. *See* LEVELUP, https://www.thelevelup.com/; *see also, e.g.*, *Sweetgreen app*, APPLE ITUNES PREVIEW, https://itunes.apple.com/us/app/sweetgreen/id594329490 (explaining that "[f]or every $99 you spend using the app, you'll get $9 toward your next purchase.").

A. Existing Regulations Provide Robust Protections to Mobile Payments and Should Not Be More Extensively Regulated.

Federal regulators have consistently stated that existing financial services regulations apply to mobile banking and mobile payments.[133] Consumer protections for mobile payments are dependent on the payment instrument (i.e., credit or debit card) and not based on whether the instrument is used in person or on a mobile device.[134] As a result, consumers are granted the same protections for fraud and unauthorized transactions as those existing for a physical credit or debit card transaction. Generally speaking, if a cardholder experiences an unauthorized transaction or has a dispute with a merchant, the cardholder can dispute the charge with the credit card issuer, and this ability to dispute applies to card payments made via a mobile device. Furthermore, merchants that accept Visa and MasterCard must agree to the operating terms and conditions.[135]

So far, regulators have taken a wait-and-see approach, which is appropriate here. Payments made through a digital wallet should be treated the same as payments made with a physical credit or debit card. The statutory and regulatory systems currently in place to provide consumers with protections for electronic payments are robust and ensure that consumers have limited liability for fraudulent transactions while also ensuring that consumers are provided with detailed disclosures. A consistent regulatory approach to transactions by card, regardless of whether by swipe, website, or mobile transaction, is beneficial to consumers, merchants, and processors alike; a separate regulatory scheme would cause confusion—particularly if the processing and billing are treated the same.

Digital wallets, like Apple Pay and Google Wallet, are different from money transmitters, like PayPal, that are subject to state-level money transfer rules. Digital wallets hold funds and should not be considered third-party intermediaries that transfer the funds. Digital wallets simply facilitate payments and are mechanisms for using existing processes for credit, debit, or prepaid card transactions. As such, the transactions carry no more risk of loss or fraud than physical credit or debit card purchases. Additionally, consumers who use mobile wallets are likely to receive the purchased items immediately upon completion of the point-of-sale transactions.

Digital wallets are generally linked to credit or debit cards and do not charge back to a customers' wireless bill. Unless the product structure is changed to allow for direct charges to phone bills, digital wallets will generally not fall under FCC jurisdiction. The wireless carrier providing

133. *The Future of Money*, *supra* note 29.

134. Hayashi, *supra* note 100, at 50.

135. VISA, VISA INTERNATIONAL OPERATION REGULATIONS (2013), https://usa.visa.com/dam/VCOM/download/merchants/visa-international-operating-regulations-main.pdf.

service to the mobile phone, however, will continue to be subject to FCC regulations such as the Truth-in-Billing rule.[136]

1. Mobile Wallets like Apple Pay and Google Wallet Should Be Treated like Traditional Payments

Payment mechanisms such as Apple Pay and Google Wallet facilitate electronic transactions that involve credit and debit cards. The card selected by the user for use in a mobile transaction is and should be afforded the same protections as a physical credit or debit card because the underlying transaction is via the card. Simply because the transaction is conducted over a new form of technology does not mean that the existing regulations do not or should not apply.

In support of this argument, the FDIC provided the following guidance:

> To date, no federal laws or regulations specifically govern mobile payments. However, to the extent a mobile payment uses an existing payment method, such as ACH or EFT, the laws and regulations that apply to that method also apply to the mobile payment. For example, a mobile payment funded by the user's credit card will be covered by the laws and regulations governing traditional credit card payments.[137]

While banks and financial institutions cannot always protect consumers from fraudulent activity by third parties, multiple regulations are in place to ensure that victimized consumers are not liable for fraud.[138]

The Electronic Funds Transfer Act (EFTA) "establishes consumer rights to a number of disclosures and error resolution procedures for unauthorized or otherwise erroneous transactions. The disclosures include upfront disclosures regarding, among other things, the terms and conditions of the EFT service and how error resolution procedures will work."[139] The

---

136. *See* SUZANNE MARTINDALE, MOBILE PAYMENTS AND ECONOMIC INCLUSION: ISSUES FOR CONSUMERS 11 (Dec. 1, 2011), https://www.fdic.gov/about/comein/MartindaleDec11.pdf. In an FDIC Presentation, the Consumers Union stated that the "FCC does not appear to have jurisdiction over mobile payments," as its "truth-in-billing" regulations apply only to "telephone services." *See id.* The FDIC echoes this in its mobile guidance, stating that Truth-in-Billing applies to wireless carriers. *Mobile Payments: An Evolving Landscape*, 9 SUPERVISORY INSIGHTS, Winter 2012, at 3, https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin12/SIwinter12.pdf. Given that most U.S. carriers no longer allow third-party charges and most current mobile payment systems use an underlying financial product as opposed to a phone bill charge, it seems unlikely that Truth-in-Billing will be applicable to mobile payments. *See id.*

137. *Mobile Payments: An Evolving Landscape*, *supra* note 136, at 8.

138. *See id.*

139. *Id.*

FDIC states that this regulation applies to mobile payments when the underlying transaction is made from a consumer's account through an electronic funds transfer (EFT), an example of which would be a purchase using a debit card.[140] As a result, mobile payment transactions using debit cards are protected under the EFTA.[141]

The Truth in Lending Act (TILA) requires creditors "to provide disclosures to consumers describing costs; including interest rate, billing rights, and dispute procedures."[142] The FDIC states that this regulation applies to mobile payments "when the underlying source of payment is a credit card" (or other credit account covered by TILA and Regulation Z).[143] Mobile payment transactions using credit cards will have their transactions protected under the TILA.

It is important to note, however, that the FDIC has stated that mobile payment systems that do not use the existing payment infrastructure, such as the traditional banking system or credit or debit cards, may not be subject to the laws and regulations for the existing infrastructure.[144] This does not mean, however, that the system would not be subject to regulation, as regulators like the FTC, FCC, and other state and federal banking regulators have jurisdiction over a variety of consumer protection matters. A practice that may not fall under FDIC purview, for example, could be payments made by text message and billed to the wireless phone bill, a practice that has been subject to high scrutiny and serious enforcement actions.[145]

Due to the complexity and sheer number of regulations surrounding payments, consumers may lack a clear understanding of their rights and responsibilities, as well as an understanding of which regulator is responsible for enforcing regulations to mobile payments. Both EFTA/Regulation E and TILA/Regulation Z rules require financial institutions to provide detailed disclosures to consumers in connection with opening accounts, and to periodically provide disclosures and updates thereafter.[146] The proposed CFPB rules relating to prepaid cards would bring prepaid cards under the EFTA and TILA, which would effectively result in requiring similar disclosures for prepaid cards.[147] While banks and financial institutions frequently use model disclosures, such as those provided by the CFPB or other banking regulators, these disclosures may still be

140. *Id.*
141. *Id.*
142. *Id.*
143. *Id.*
144. *See Id.*
145. *See, e.g*, Press Release, Fed. Trade Comm'n, T-Mobile to Pay At Least $90 Million, Including Full Consumer Refunds To Settle FTC Mobile Cramming Case (Dec. 19, 2014), https://www.ftc.gov/news-events/press-releases/2014/12/t-mobile-pay-least-90-million-including-full-consumer-refunds.
146. Truth in Lending Act, 15 U.S.C. §§ 1601-1667f (2012); *see generally* Regulation E, 12 C.F.R. § 205 (2016); Regulation Z, 12 C.F.R. § 226 (2016).
147. Prepaid Accounts under the Electronic Fund Transfer Act (Regulation E) and the Truth In Lending Act (Regulation Z), 79 Fed. Reg. 77101 (proposed Dec. 23, 2014) (to be codified at 2 C.F.R. pts. 1005, 1026).

complicated for consumers to understand.[148] Furthermore, a paper insert received in an envelope with a plastic credit card may not be easily accessible. As a result, financial companies involved with a mobile payment product should make sure that disclosures are easy to read and available online for consumers to access at any time.[149]

2. Technology Companies Do Not Necessarily Fall Under the CFPB's Supervision as a Result of Their Involvement in Mobile Payments

The Dodd-Frank Act grants jurisdiction to the CFPB over "covered persons" and "service providers," subject to a limited number of exceptions.[150] The Dodd-Frank Act gives the CFPB authority to regulate unfair, deceptive, or abusive acts or practices (UDAAP) by these entities in the course of transactions or offerings of consumer financial products or services.[151] While the scope of this authority is still yet to be clearly defined, the CFPB has asserted that it encompasses mobile payments,[152] recently stating that:

> The Bureau's role is not to choose market winners and losers, but to protect consumers and to make sure that companies offering consumer financial products or services play by the same rules. By and large, those rules are technologically neutral. Rules that apply to plastic card payments generally also apply to payments with a phone. For example, disclosures must be clear, consumers must be protected from unauthorized transactions, and conduct towards consumers must not be unfair, deceptive, or abusive.[153]

148. Eric Goldberg, *Prepaid Cards: Help Design a New Disclosure*, CONSUMER FIN. PROT. BUREAU: POL'Y & COMPLIANCE (Mar. 18, 2014), http://www.consumerfinance.gov/blog/prepaid-cards-help-design-a-new-disclosure/.

149. Note that the FTC issued a study on mobile shopping apps in 2014 that found that app disclosures were lacking and did not provide consumers with important information relating to payment disputes and consumer data. *See* Press Release, Fed. Trade Comm'n, Staff Report on Mobile Shopping Apps Found Disclosures to Consumers Are Lacking (Aug. 1, 2014), https://www.ftc.gov/news-events/press-releases/2014/08/staff-report-mobile-shopping-apps-found-disclosures-consumers-are. While mobile shopping apps are different from mobile payments, *see supra* Section II.B, it would not be out of the question for regulators to examine mobile payment disclosures as well, particularly given the challenges involved with limited screen space.

150. 12 U.S.C. § 5481 (2012).

151. *See* Dodd-Frank Wall Street Reform and Consumer Protection Act §§ 1031, 1036(a), 12 U.S.C. §§ 5531, 5536 (2012).

152. *See* Douglas-Gabriel, *supra* note 113; *see also* Dunn, *supra* note 113.

153. Dunn, *supra* note 113 (quoting the remarks of Moira Vahey, CFPB spokesperson).

While it is accurate to say that the technologically neutral rules applying to physical card payments also apply to mobile payments,[154] tech companies involved with mobile payments should not be responsible for unfair, deceptive, or abusive conduct resulting from card issuers' or financial institutions' unilateral decisions. For example, if a bank's conduct relating to the advertising of a credit or debit card was found to run afoul of CFPB's UDAAP authority, that does not necessarily mean that the technology provider like Apple Pay or Google Wallet should also be found liable of UDAAP as a result of facilitating a transaction associated with the violating card.

The FDIC reiterates this stance on the application of these consumer protection laws and provides guidance, stating that the CFPB's UDAAP authority and the FTC's UDAP authority "applies to all mobile payments regardless of underlying payment source."[155]

Taking the contrary position, Georgetown University Law Center Professor Adam Levitin argues that "[c]ard issuers are covered persons, and Apple is providing a material service in connection with a consumer financial product: a credit card."[156] Consequently, Levitin argues that Apple has become a "regulated financial institution."[157] Levitin argues that Apple's involvement (as well as Google's) hinges on their "participat[ion] in designing, operating, or maintaining [a] consumer financial product or service."[158] In a blog post on the topic, Levitin distinguishes Apple's involvement and says that, while the device (i.e., hardware) does not trigger CFPB supervision, Apple's development of the Apple Pay feature means that Apple Pay is operating and maintaining a payment system.[159]

This interpretation of the CFPB definition is problematic. If Apple (or Google as the provider of Google Wallet) is considered a financial provider, it may gain responsibility of providing fraud protection, limited liability and other services traditionally provided by banks, payment processors, and other financial institutions. This interpretation of Apple as a service provider would mean that there would be overlapping jurisdictions and multiple layers of regulated institutions. This is a regulatory burden that does not benefit the consumer because the Apple Pay product uses existing payment infrastructure that is already sufficiently regulated. The bank or financial institution issuing the underlying payment method—which is likely a credit, debit, or prepaid card—is and should be subject to applicable regulations and CFPB supervision.[160]

The potential for the interpretation of Apple or similar companies as a "service" provider has not gone unnoticed by the CFPB. In a September

154. *See id.*

155. *Mobile Payments: An Evolving Landscape*, *supra* note 136.

156. Dunn, *supra* note 113.

157. Adam Levitin, *Apple Pay and the CFPB*, CREDIT SLIPS (Sept. 10, 2014, 10:56 PM), http://www.creditslips.org/creditslips/2014/09/apple-pay-and-the-cfpb.html.

158. *Id.*

159. Dunn, *supra* note 113.

160. See 12 U.S.C. §§ 5531, 5536, 5481 (2012).

2014 speech, CFPB Director Richard Cordray stated that the CFPB had sent Requests for Information on issues relating to mobile banking and financial management services to address potential consumer protection issues.[161] Director Cordray then made general remarks about mobile payments, stating that:

> Using mobile devices for all sorts of banking services can make some transactions cheaper or faster or both. But we need to make sure that the legal and regulatory framework can keep up effectively, so that all consumers can be well served and remain protected, whether they are opening their wallet or scanning the screen on their smartphone.[162]

The CFPB issued a report on mobile financial services in November 2015 based on the results of its Request for Information,[163] but it remains uncertain what other actions the agency might take in this space.

B. Even Without Existing Regulations to Ensure Consumer Protection, Products like Apple Pay and Google Wallet Are Designed for Security

In addition to being subject to existing statutory and regulatory protections for traditional payments transactions, many of the emerging payment technology mechanisms and products have been developed to ensure that transactions are safe and secure. These increased security measures are an essential step in ensuring that consumers are comfortable adopting a new technology, especially due to the frequency of data breaches and the subsequent burdens involved with remedying the consequences of these data breaches. At the heart of a mobile payment is the smartphone itself and its unique profile of features, such as Wi-Fi, GPS data, and the type and number of apps.[164] This unique profile can help the device identify whether the user is authentic and can erect barriers if the purchase seems suspect or fraudulent.[165] Additionally, many mobile payments take advantage of encryption technology to ensure secure payments.[166]

Apple, for example, has implemented several security protections for its Apple Pay product. First and foremost, in order to use the device, a user

---

161. Darrell Delamaide, *Delamaide: Apple Pay May Test Regulators*, USA TODAY (Sept. 16, 2014, 8:44 PM EDT), http://www.usatoday.com/story/money/business/2014/09/16/delamaide/15743653/.

162. *Id.*

163. CONSUMER FIN. PROT. BUREAU, MOBILE FINANCIAL SERVICES (2015), http://files.consumerfinance.gov/f/201511_cfpb_mobile-financial-services.pdf.

164. *See* Moulds, *supra* note 116.

165. *Id.*

166. *See, e.g.*, PCI SEC. STANDARDS. COUNCIL, ACCEPTING MOBILE PAYMENTS WITH A SMARTPHONE OR TABLET (2014), https://www.pcisecuritystandards.org/documents/accepting_mobile_payments_with_a_smartphone_or_tablet.pdf.

must enter a passcode and choose to set up a fingerprint verification (Touch ID).[167] Then, in order to use the Apple Pay feature, the user must link a credit or debit card to his or her Apple account.[168] The credit or debit cards that are used for payment are subject to the aforementioned regulations and are also subject to additional security measures put in place by Apple.[169] When entering credit card details, a user can use the device's camera or type in the numbers.[170] In either case, the information is encrypted.[171] According to Apple:

> If you use the camera to enter the card information, the information is never saved to the device or stored to the photo library. Apple decrypts the data, determines your card's payment network, and re-encrypts the data with a key that only your payment network can unlock. Then it sends the encrypted data, along with other information about your iTunes account activity and device (such as the name of your device, its current location, or if you have a long history of transactions within iTunes) to your bank. Using this information, your bank will determine whether to approve adding your card to Apple Pay.[172]

After the credit or debit card is approved, the payment network or the consumer's bank creates a unique Device Account Number.[173] This Number is also encrypted, and Apple is unable to decrypt this number. Instead, Apple will add it to the Secure Element within the consumer's device.[174] Apple describes Secure Element as:

> An industry-standard, certified chip designed to store your payment information safely. The Device Account Number in the Secure Element is unique to your device and to each card added. It's isolated from iOS, never stored on Apple Pay servers, and never backed up to iCloud. Because this number is unique and different from usual credit or debit card numbers, your bank can prevent its use on a magnetic stripe card, over the phone, or on websites.[175]

Google highlights similar protections for its Google Wallet product, including one-hundred percent fraud protection, ability to disable the

167. *Apple Pay Security and Privacy Overview*, APPLE (last modified May 6, 2016), http://support.apple.com/en-us/HT203027.
168. *See id.*
169. *See id.*
170. *See id.*
171. *See id.*
172. *Id.*
173. *See id.*
174. *See id.*
175. *See id.*

account if the mobile device is lost or stolen, a custom four-digit PIN, transaction notifications, and data encryption.[176] Whether these security precautions for mobile devices will be effective, however, remains to be seen. Experts take both sides on whether the system is as secure as the developer claims it to be, but it is possible that the tokenization technology will make mobile payments more secure than the traditional card swipe that leaves card data less secure and more at risk in the event of a breach. While some argue that mobile payments may not be foolproof with respect to security from hackers, others argue that Apple Pay takes the essential step of eliminating the use of the old credit card number storage format, which raised significant risks when major companies and retailers were breached in recent months.[177] Robert Neivert, chief operating officer of Private.me, a company that created an anonymous search engine and is working to improve online privacy, says that, while "nothing is absolutely secure," Apple's elimination of the old card format is "an improvement from the existing [options.] . . . It takes away one of the most prominent ways in which security breaches happen, which is intercepting that credit card number."[178]

There have been reports of fraudulent transactions occurring on Apple Pay, specifically a series of transactions occurring at Apple retail stores using stolen credit card numbers.[179] While this may be concerning to some and call into question the security of the Apple Pay system, these incidents are not a result of an Apple Pay breach, but instead are legacy problems resulting from previous data breaches at retailers such as Home Depot and Target.[180] Fraudsters were able to make unauthorized purchases without having a physical card present by instead using stolen card numbers in the Apple Pay system.[181] Banks and card issuers alerted to this problem have, as a result, made changes to tighten their verification procedures for inserting card data for use with Apple Pay.[182] While this is an example of a potential flaw to the mobile payments system, the quick reaction of companies to address the weakness is a testament to the commitment to the security and success of mobile payments. Additionally, it is likely that these types of fraudulent transactions will decrease as tokenization becomes more popular, resulting in fewer usable credit or debit card numbers in circulation following a breach.

176. *See Google Wallet*, GOOGLE, https://www.google.com/wallet/ (last accessed Mar. 2, 2016).

177. *See, e.g.*, Louis Bedigian, *Is Apple Pay Secure?*, YAHOO! FIN. (Oct. 24, 2014, 10:08 AM), http://finance.yahoo.com/news/apple-pay-safe-140843948.html.

178. *Id.*

179. Robin Sidel & Daisuke Wakabayashi, *Apple Pay Stung by Low-Tech Fraudsters*, WALL ST. J. (Mar. 5, 2015, 7:50 PM ET), http://www.wsj.com/articles/apple-pay-stung-bylow-techfraudsters-1425603036.

180. *Id.*

181. *Id.*

182. *Id.*

V. CONCLUSION

Convincing consumers to switch from cash or a traditional credit card swipe to a new mobile payment technology may take time, as consumers have concerns about the security and privacy of mobile payments. In reality, however, mobile payments use advanced technologies like tokenization to ensure safety of payment data. Additionally, transactions through mobile payments are protected through underlying regulations that provide consumer protections for credit, debit, and prepaid card transactions. New mobile payment mechanisms are designed to work within the existing payment infrastructure and are consequently protected by existing regulations. While it is prudent to monitor the mobile payments space to ensure that consumers are adequately protected by current laws, additional regulations for mobile payments are likely unnecessary and overly burdensome and could stifle innovation and product development.