BREAKING BENJAMIN: SECURITY THREATS IN MOBILE PAYMENT APPLICATIONS

NOLAN MURRAY*

I. INTRODUCTION

An efficient method of payment is critical to the success of any economic system. Over the past millennium, the transitions from bartering to precious metal currency and subsequently from precious metals to paper bank notes have each spurred enormous growth in global economic activity.[1] Not only has each evolution empowered more people to enter the economic system, but also it has caused participants to transact in greater volume and with a larger number of trading partners.[2]

The latest and current evolution of the global economy is the adoption of web-based payment platforms.[3] Initially, these only took place through a traditional web browser on standard desktop computers between customers and merchants.[4] However, with the advent of smartphones and the development of social media, in conjunction with the stunning progress of developers in Silicon Valley, buyers and sellers can now participate in transactions anywhere cellphone coverage or Wi-Fi is available.[5]

Furthermore, web-based financial activity is no longer limited to transactions between a business and a customer, as individuals can also conduct financial exchanges with each other.[6] Conceptually, the line demarcating transactions with traditional big-box retailers, small businesses and those among friends for shared expenses has become difficult to draw.[7] This evolution has spawned an entirely new technological sector for simple,

[*] *Juris Doctor Candidate,* The Ohio State University Moritz College of Law, May 2018. I would like to thank my family, for their unwavering support, friends, for assuring me there is a world beyond law school, and coffee, for the late night encouragement.

[1] *See* Andrew Beattie, *The History of Money: From Bartering to Banknotes,* INVESTOPEDIA, http://www.investopedia.com/articles/07/roots_of_money.asp (last visited Feb. 21, 2017).

[2] *Id.*

[3] *Id.*

[4] Dr. Fiona Ellis-Chadwick, *History of Online Retail,* The Open University, http://www.open.edu/openlearn/money-management/management/business-studies/history-online-retail (last visited May 9, 2017).

[5] Square Guide, *What are Mobile Payments?,* SQUARE (Last visited May 9, 2017), https://squareup.com/guides/mobile-payments

[6] *Id.*

[7] *Id.*

quick and inexpensive monetary transfer applications.[8] This paper will argue that the law has been slow to develop the rules and regulations sufficient to strengthen the security features of these platforms and necessary to instill confidence in consumers.

The largest players in the mobile payment sector come from both familiar technology giants and unheralded startups.[9] The relatively small capital requirements for developing mobile payment systems have allowed small companies to quickly access the market and become widely adopted.[10] Some of the most popular of these technologies include Apple Pay, Google Wallet, PayPal, Venmo and Square Cash.[11] Future Market Insights estimates that transactions conducted in this market will total $2.8 trillion by 2020.[12] As new technology continues to pour into the market, the "per transaction" fees of these services, which had historically been a major hurdle to widespread adoption, will continue to drop.[13] In turn, the gradual removal of financial barriers will enable more people to adopt the technology.

The simplicity and speed of transactions on mobile devices has undoubtedly provided additional incentives for the adoption of mobile payment technology. Studies have estimated that mobile payment technology can be fifteen to thirty seconds faster than swiping a credit or debit card and signing or entering a PIN.[14] The ubiquitous presence of smartphones and omnipresent availability of high-speed Internet have helped usher in this new era of payment by placing a device within reach of nearly all market participants.[15]

The mobile payment industry has a huge advantage as the hardware is already in the hands of most of its users, the industry only needs to

[8] *Id.*

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

[10] *Id.*

[11] Christian de Looper, *PayPal vs. Venmo vs. Square vs. Google: Who Makes the Best App for Sending Cash?*, DIGITAL TRENDS (July 8, 2016), http://www.digitaltrends.com/mobile/paypal-vs-google-wallet-vs-venmo-vs-square-cash/.

[12] *ISACA Survey: 87% of Cybersecurity Experts Say Mobile Payments Data Breaches Will Grow, Yet 42% Report Using this Payment Method,* ISACA (Sept. 24, 2015), https://www.isaca.org/About-ISACA/Press-room/News-Releases/2015/Pages/isaca-survey-mobile-payments-data-breaches.aspx [hereinafter *ISACA Survey*].

[13] *Id.*

[14] Carolyn Lowry, *What's in Your Mobile Wallet? An Analysis of Trends in Mobile Payments and Regulation*, 68 FED. COMM. L.J. 353, 373 (2016).

[15] Aaron Smith, *Record shares of Americans now own smartphones, have home broadband,* PEW RESEARCH CENTER (Jan. 12, 2017), http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/.

convince users to download inexpensive, or free, software.[16] Already, smartphones have replaced many everyday items, including alarm clocks, watches, cameras and laptop computers.[17] Soon, this list may include cash, physical credit cards and even wallets.

A March 2011 survey found that nearly one in five Americans with both a bank account and a mobile phone had used his or her phone to conduct banking with a financial institution within the previous ninety days.[18] Access to mobile technology is already present in most American households, which indicates that the infrastructure for and social acceptance of the technology is present.[19]

Adoption rates amongst younger Americans are likely to further buoy the potential for the growth of mobile payments in the United States. Millennials, who have known mobile technology since childhood, are likely to be very comfortable using a bank's mobile app or completing checkout at a retailer with their phone. One study found that of the ninety million millennials worldwide, some forty million would switch to a digital-only bank.[20]

However, a major challenge for the mobile payment industry is ensuring that strong, transparent security features effectively accompany growth. A potentially formidable obstacle to the widespread use of mobile payment technology are consumer concerns. Many people remain worried about data breaches impairing their financial security and privacy.[21] John Pironti, a risk advisor for the mobile payment technology industry group Information Systems Audit and Control Association ("ISACA") and president of IP architects noted, "mobile payments represent the latest frontier for the ongoing choice we all make to balance security and privacy risk and convenience."[22] Successfully navigating the tension between these competing goals will be a key for allowing this technology to deliver maximum benefits to the economy.

[16] *Id.*

[17] Jonathan Reinisch, *Swipe Freeze: How The "Durbin Amendment" is Preventing your Mobile Phone from Replacing your Wallet,* 63 DEPAUL L. REV. 123, 130 (2013).

[18] *Id.* at 130.

[19] *Id.*

[20] Will Hernandez, *From the source: Millenials share views about Alexa, Apple Pay, Venmo,* MOBILE PAYMENTS TODAY (Sept. 23, 2017), https://www.mobilepaymentstoday.com/blogs/from-the-source-millennials-share-views-about-alexa-apple-pay-venmo/

[21] *ISACA Survey*, *supra* note 12.

[22] *Id.*

This paper analyzes the growth of the mobile payment industry, the present security concerns of both merchants and consumers, and how the law currently affects this industry. It also discusses factors the law should consider in to help promote growth and stability for customers and how the legal system is as an effective tool for shaping a strong regulatory environment that promotes security while enabling technological advancement. A concern that will be present throughout this paper is whether the enactment of legislation and regulation can keep up with the breakneck speed at which technology develops.

II. HISTORY OF MOBILE PAYMENTS

To understand the current landscape of the mobile payments industry, it is necessary to understand the history and development of mobile payment technology. "Mobile payment" is an umbrella term that refers to a wide variety of different types and forms of transactions.[23] However, what mobile payments all have in common is the use of the consumer's credit or debit card for the underlying payment.[24] Consumers may use the web browser of a mobile device, a text message, a mobile application, or through a point-of-sale or Near Field Communication transaction.[25] The myriad of methods and terminology has been an obstacle in the industry for many years, which has proven to be a difficult hurdle, as businesses, consumers and developers have not coalesced around one common technology.[26]

Uncertainty and continuous evolution are not new however, as the technology has been around for nearly twenty years.[27] Mobile payments first gained notoriety in 1997, when Nokia allowed customers to use short messaging service ("SMS") text messaging to purchase drinks from Finnish vending machines.[28] However, it is believed that the first web based payment occurred in 1994 with the order of a pizza from Pizza Hut.[29] Mobile payments are payments "where a mobile device is used to initiate, authorize, and confirm an exchange of financial value in return for goods and services."[30] This broad definition, therefore, includes transactions carried out through applications on mobile devices as well as payments made through the Internet browser of a Smartphone that mirror those made on a desktop computer.

[23] Square Guide, *supra* note 5.
[24] Lowry, *supra* note 14, at 380.
[25] *Id.* at 360.
[26] Rampton, *supra* note 9.
[27] Reinisch, *supra* note 17, at 133.
[28] *Id.*
[29] Rampton, *supra* note 9.
[30] Reinisch, supra note 17, at 130.

Mobile payments consist of two broad categories.[31] The first, known as remote payment, allows consumers to use a phone equipped with either SMS or wireless application protocol ("WAP") technology to send a payment to a merchant or individual.[32] This technology requires consumers to link a bank account or credit or debit card to an account connected to a mobile-payment service provider ("MPSP").[33] Consumers can then make a payment by sending a text message to the MPSP stating the amount of money to transfer and to which destination to send the money.[34] Websites using this technology allow consumers to access a merchant's website using a mobile device and make a purchase directly on that website.[35] This type of payment can also be used as a virtual, preloaded gift card that appears on a consumer's phone.[36] One example of this technology is the Starbucks mobile payment application, which was initially launched in 2011.[37] On the app, customers link their personal credit or debit card to a virtual gift card on the app, which in turn is used to complete purchases.[38]

The second broad category of mobile payment technology is proximity payment.[39] This technology employs near field communication ("NFC") technology, which allows consumers to make purchases simply by waving their phone in front of an NFC-equipped terminal.[40] Conceptually, these transactions are similar to traditional credit or debit cards.[41] At the point of payment, the consumer's phone will access the synced financial account and send the data to the merchant's acquiring bank.[42] That bank then sends the transaction data to the customer's bank, which authenticates and authorizes the transaction.[43] This technology allows consumers to skip the step of removing physical cards or cash and streamlines the checkout process for retailers.

Estimates suggest that ninety-one percent of the U.S. population has a cellphone capable of utilizing at least one form of mobile payment technology.[44] Therefore, a large audience awaits merchants and banks that can successfully deploy this technology. One of the greatest potential benefits of this technology is the reduction of transaction costs between

[31] *Id.*

[32] *Id.* at 130-31.

[33] Reinisch, *supra* note 17, at 131.

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] *Id.* at 135.

[38] Reinisch, *supra* note 17, at 135.

[39] *Id.* at 131.

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] Reinisch, *supra* note 17, at 131.

[44] *Id.* at 130.

consumers and businesses, which could deliver significant economic benefits by allowing for more efficient interactions.[45] For example, within two years of launching its mobile payment app, Starbucks reported that 25% of its sales took place on the app, which lowered credit card fees and reduced cash handling cost.[46]

Additionally, consumers are beginning to buy into the technology en masse. For example, in the third quarter of 2014, Venmo, a subsidiary of PayPal, processed $700 million in payments—nearly five times the transaction volume it did during the same period a year earlier.[47] Further, Venmo, which allows users to transfer payments between one another directly without using an intermediary bank, known as peer-to-peer, has become omnipresent on college campuses.[48] This technology, and its competitor Square Cash, is especially popular on college campuses and with young professionals.[49] As eBay chief executive John Donahoe noted, "If you go to any college campus across America, they talk about Venmoing money to each other."[50] Despite the potential for identity theft or fraud, this demographic is the largest adopter of this technology, as 45% of those aged 18-34 has made an NFC payment.[51]

Currently, millennials control only a small portion of the financial markets.[52] However, as this cohort ages, its influence and market power will lead it to dominate the economy.[53] Millennials are also attracted to other features of mobile payment technology, such as the ability to conveniently track and record purchases.[54] This can help eliminate the needs for receipts, allow for more frequent tracking of expenses and eliminate the need to balance a checkbook by hand.[55] Furthermore, mobile payment technology is also beneficial to merchants because it can help build brand loyalty by

[45] *Benefits of Mobile Payments,* CENTRE FOR ECONOMICS AND BUSINESS RESEARCH (Mar. 24, 2017), https://www.cebr.com/reports/benefits-of-mobile-payments/.
[46] Reinisch, *supra* note 17, at 135-36.
[47] Alison Griswold, *Venmo Money, Venmo Problems,* SLATE (Feb. 25, 2015), http://www.slate.com/articles/technology/safety_net/2015/02/venmo_security_it_s_not_as_strong_as_the_company_wants_you_to_think.html.
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] *Nearly half of millennials have used a mobile wallet,* BUSINESS INSIDER (Sept. 6, 2016), http://www.businessinsider.com/nearly-half-of-millennials-have-used-a-mobile-wallet-2016-9.
[52] Richard Fry, *Millennials overtake Baby Boomers as America's largest generation,* PEW RESEARCH CENTER (Apr. 25, 2016), http://www.pewresearch.org/facttank/2016/04/25/ millennials-overtake-baby-boomers/.
[53] *Id.*
[54] Reinisch, *supra* note 17, at 134.
[55] *Id.*

incentivizing consumers to use their payment app.[56] These programs often present rewards or discounts to consumers who use mobile technology, which can boost sales and improve customer satisfaction.[57]

However, as with any developing technology, mobile payments are not without their risks. In a recent article, TIME Magazine described some of the grave dangers posed by Venmo.[58] The company processed $2.4 billion worth of payments in 2014.[59] However, the company has taken heat for lacking in customer service.[60] Furthermore, Venmo only recently added a two-factor authentication system.[61] The company only made this change after receiving a multitude of complaints over the lack of security in prior versions of its app.[62] Two-factor authentication requires users to verify additional information after entering their personal password.[63] Examples of the second authentication factor include personal security questions or a code sent to the phone via text message.[64] Mobile security experts believe that two factor authentication is a wise preventative measure to prevent the theft of important financial or personal information.[65]

Another major issue for mobile payment technology is the delay in processing cash transfers.[66] Many people use mobile payment technology to conduct business with friends and strangers alike, and assume that deposits are made the moment the transaction is completed on the app.[67] However, it often takes at least one business day before the funds are deposited into the account of the recipient.[68] This can create problems for those who maintain a relatively thin bank account balance and are unaware of this lag. Additionally, this delay may also allow thieves time to withdraw funds from their own account before the mobile payment application removes and transfers the funds.[69] Conceptually, this is similar to a check written with

[56] *Id.* at 136.

[57] *Id.*

[58] Ethan Wolff-Mann, *The Scary Thing You Don't Understand About Venmo,* TIME, INC. (Sept. 21, 2015), http://time.com/money/4036511/venmo-more-check-than-cash/.

[59] *Id.*

[60] *Id.*

[61] *Id.*

[62] *Id.*

[63] *Are Mobile Payment Apps Safe?,* THE HUFFINGTON POST (July 17, 2016),http:// www.huffingtonpost.com/comparecards/are-mobile-payment-apps s_b_7819278.html.

[64] *Id.*

[65] *Id.*

[66] *See* Wolff-Mann, *supra* note 58.

[67] *Id.*

[68] *Id.*

[69] *Id.*

insufficient funds present, and may leave the recipient with few options for recourse.[70]

III. New Developments in Mobile Payment Technology

As the mobile payment scene continues to evolve to meet experiential and security concerns, observers are paying increased attention to the smallest changes and developments of each application. Recently, PayPal introduced a system at 3,000 retail locations that enables customers to enter a mobile phone number and PIN into a retailer's point of sale system to complete a purchase.[71] Unfortunately, this system still requires processing through PayPal, which requires the customer to have an existing PayPal account.[72] The cumbersome nature of this process may prove to be too difficult a hurdle to overcome to achieve widespread consumer adoption.

Another competitor, Square Cash, has recently unveiled plans to integrate a GPS tracking system into its application.[73] This system would allow consumers to complete a purchase at a store after the retailer enters the sale into the checkout system and determines that the payment platform is present with the consumer in the store.[74] Before this new product development, the primary use for Square was transferring funds between individuals. Square's early success has been attributed to its ability to offer a free payment processing application and credit card processing hardware for only $10.[75] In this function, it is similar to SnapCash (from Snap Chat), Facebook Cash (from Facebook) and Venmo, where users could make payments to one another, but not to major retailers.

The federal government has recently integrated Apple Pay into its federal payments cards, which opens the door for future widespread adoption within the government.[76] For this program to be successful, the technology will need to remain both secure and widely available to millions of Americans. However, widespread adoption presents a major hurdle in the process of achieving mass integration of mobile payment technology into everyday life for ordinary Americans due to privacy and data security concerns.[77] On the other hand, if the federal government adopts Apple Pay or a similar payment processer, it could use this technology to deliver social

[70] *Id.*
[71] Reinisch, *supra* note 17, at 133.
[72] *Id.*
[73] *Id.* at 133-34.
[74] *Id.* at 134.
[75] Everette Taylor, *Square – How Did Square Grow So Quickly?,* GROWTH HACKERS, *https://growthhackers.com/growth-studies/square* (last visited Mar. 21, 2017).
[76] Lowry, *supra* note 14, at 373.
[77] *Id.* at 372-73.

security benefits to the fifty-six million Americans enrolled in that program.[78] With this integration, Apple Pay's users would drastically increase.[79] This program could potentially save millions of tax dollars by reducing transactions and delivery costs.

Another system for processing payments with a mobile device is the use of host card emulation ("HCE"). Previously, there were only two different possibilities for securing customer payment credentials in mobile transactions: Secure Element and Card on File.[80] Secure Element is essentially a virtual wallet in which important data is kept on the phone and then transmitted to an EMV card.[81] Card On File was the equivalent of maintaining relevant payment information in the cloud.[82]

Today, many companies instead use a different form of HCE technology, known as an Application Program Interface ("API").[83] This technology creates a payment profile on the merchant's payment processor and uses a token to verify the authenticity of the customer.[84] The API can be reused several times to help reduce payment processing time and ensure the secure transmission of vital customer information.[85] While HCE undoubtedly provides many benefits for consumers, there are inherent risks, including identity theft, fraud and privacy concerns.[86] Experts have expressed worry that if these concerns are not properly addressed, hackers might be able to reverse engineer portions of the sensitive code information that transmits or processes encryption keys within the mobile devices to obtain the sensitive information of consumers.[87]

As these systems have become increasingly complex, many companies lament the difficulties of involving multiple levels of hardware

[78] *Id.* at 374.
[79] *Id.*
[80] Richard Moulds, *Why Mobile Payments Adoption Has Been Slow – And Why That's About to Change,* WIRED, https://www.wired.com/insights/2015/01/mobile-payments-adoption/ (last visited Jan. 8, 2017).
[81] *Id.*
[82] *Id.*
[83] Vangie Beal, *API – application program interface,* WEBOPEDIA, http://www.webopedia.com/TERM/A/API.html (last visited May 10, 2017).
[84] Robert Brodie, *The problems weighing down mobile payments,* MOBILE PAYMENTS TODAY (Apr. 26, 2016), http://www.mobilepaymentstoday.com/articles/the-problems-weighing-down-mobile-payments/.
[85] *See id.*
[86] Thorston Held, *Recent POS malware attacks signal a need for app security for mobile payments,* MOBILE PAYMENTS TODAY (Sept. 13, 2016), https://www.mobilepaymentstoday.com/articles/recent-pos-malware-attacks-signal-a-need-for-app-security-for-mobile-payments/.
[87] *Id.*

and software in their payment systems.[88] The development and integration process, known as Microservice architecture, stresses the importance of carefully planning each piece of the system to ensure sufficient level of failover and separation.[89] Companies that carefully plan and implement new technology will be able to avoid duplicating costs and effort, while delivering significant value to their customers.

IV. History of Data Breaches

As consumers and retailers flock to mobile payment systems, there is a need to ensure that thieves and hackers are not able to take advantage of the naivety of new consumers. Experts favor two-factor authentication systems or short-term authentication codes far more than the installation of additional security applications on their mobile phones.[90] In 2015, a report by the global cyber security association ISACA found that security threats are unlikely to deter people who utilize mobile payment systems.[91] This could be alluring to potential thieves who are looking for naïve, unsuspecting targets to swindle cash or steal personal information.

Furthermore, a recent study by the global professional services firm KPMG found that 56% of consumers trusted their financial institution with their payment data, while just 6% would place that same level of trust in their mobile and internet service providers.[92] This sharp divide could be a point of alarm for the industry but particularly for retailers and mobile phone service providers, who are seeking to attract mainstream consumers.

Part of the reason there are no unified security protocols is because the industry lacks a standard for which entity, between the consumer, the retailer, and the bank, is responsible for keeping mobile payments secure.[93] One form of security guidance is the COBIT governance framework.[94] This system encourages all key stakeholders to decide upon a relationship that appropriately balances fraud rate and revenue.[95] However, the vast amount of negotiation and collaboration required for this conceptual framework may hinder implementation. Furthermore, without legal requirements, an industry backed theoretical model may only have limited success, as it will lack sufficient teeth through an enforcement mechanism.

[88] *See* Brodie, *supra* note 84.
[89] *Id.*
[90] ISACA Survey, *supra* note 12.
[91] *Id.*
[92] Reinisch, *supra* note 17, at 132.
[93] ISACA Survey, *supra* note 12.
[94] *Id.*
[95] *Id.*

In recent years, massive data breaches that have received significant publicity have rocked the mobile payment industry. Consumers remain concerned about the data breaches at high-profile retailers in recent years, which have resulted in the theft of customer data.[96] Consumers might be wary about trusting these institutions with sensitive information.[97] This lack of trust among existing consumers may result in irreversible reputational damage.

Some of these issues may be self-inflicted wounds due to the lack of quality control and customer interaction. For example, Venmo does not alert account holders if the email address or password credentials associated with the account are changed.[98] This creates a wide window for a hacker to seize the information, quickly make purchases or cash transfers and drain the bank account of the victim.[99] Furthermore, the social-networking aspect of the Vemno app poses additional risks as thieves may pose as a friend or relative to request or receive money.[100] Consumers may be less likely to question a request from an account posing as a friend or relative when in fact, the username is slightly changed, the profile image is stolen, and a thief is behind the account.

For security developers, the battle to stay one-step ahead of hackers comes with no respite. As security holes are blocked and new technology is developed, hackers' attacks continue to become more sophisticated and insidious.[101] Many new attacks come via complex frauds designed to steal passwords from consumers, similar to phishing frauds perpetuated through email.[102] A notable version of these frauds is DarkSideLoader.[103] This program operates by loading software onto the target device before stealing vital information from the host.[104] The similar appearance of these programs to legitimate software poses danger for consumers because it is difficult to decipher the authentic program.[105] Once downloaded thieves can capture the vital information necessary to hack the accounts and privacy of the targets.[106]

[96] Moulds, *supra* note 80.
[97] *Id.*
[98] Griswold, *supra* note 47.
[99] *Id.*
[100] *Id.*
[101] *See* Oren Kedem, *Through the mobile maelstrom: What app makers owe their customers*, MOBILE PAYMENTS TODAY (July 26, 2016), http://www.mobilepaymentstoday.com/ articles/through-the-mobile-maelstrom-what-app-makers-owe-their-customers/.
[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] *Id.*
[106] Kedem, *supra* note 101.

Most often, these applications appear as a free version of a popular game–however, inside the application lurks malicious code.[107]

Insufficient customer support after an account has been hacked has resulted in distrust and security concerns, which could lead to stunted growth of the mobile payment industry.[108] For example, as of November 2014, Venmo only had seventy full-time employees and did not have a phone line for customer service.[109] Venmo has also come under fire for its extremely slow response time to emails and complaints regarding stolen funds.[110] Although Venmo claims to have security on par with major banks, it still does not offer two-step verification.[111] Two-step verification "requires users to provide a secondary pass code to access an account."[112] However, Venmo does limit liability to $50 for the loss or theft of funds; however, that liability limit jumps to $500 if customers do not contact the company within two business days of discovering the loss.[113] For those that do not check their bank accounts on a daily basis, this policy could expose them to vast risks of loss to criminals.

The lack of consumer confidence in mobile technology mirrors the concerns of industry experts.[114] In a recent survey, only 23% of respondents thought that mobile payment systems were secure, while 87% of industry experts believed that the number of mobile-payment data breaches would increase in 2016.[115] Frauds and other hacking programs are a significant threat to consumers; however, the most dangerous threats may come from seemingly innocuous daily activities. A study by ISACA found that the use of public Wi-Fi on a payment-enabled device, lost or stolen devices, and phishing were experts' top concerns for increasing data reaches.[116]

From a consumer standpoint, the convenience and social aspects of mobile payments may outweigh the security shortcomings, which could encourage some consumers to use the service. One of the most popular aspects of Venmo is the ability of users to view the transaction history of their social media friends.[117] Venmo is integrated with Facebook, so users

[107] *Id.*

[108] Griswold, *supra* note 47.

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] Griswold, *supra* note 47.

[113] *Id.*

[114] *Mobile Payments Security: Perceptions and Behaviors*, ISACA, http://www.isaca.org/SiteCollectionDocuments/CSX-Mobil-Payment_whp _eng_0915.pdf (last visited Feb. 4, 2017) [hereinafter *Mobile Payments Security*].

[115] *Id.*

[116] *Id.*

[117] Griswold, *supra* note 47.

are not only able to see who has paid whom, but also can "like" and comment on the transactions of friends.[118] However, the social media functions of Venmo may put users at ease regarding security, which could make them vulnerable to hackers. In a recent paper, three students from the Massachusetts Institute of Technology warned, "Venmo's interface and social-networking component made it vulnerable to 'social engineering attacks.'"[119] Not only can hackers steal information, but thanks integration with Facebook, it may also be possible to gather crucial clues about the location, friends, and activities of the victim, which could enable the thief to broaden the impact of their attack.[120]

Industry experts offer several simple steps that may help limit the ability of hackers to attack the user's accounts, many of which are simple and intuitive options that can help to reduce the risk of harm from a hacker. First, experts encourage the use of secure passwords.[121] This includes merchants, who may have purchased commonly used point of sale systems that may have a preset password for the new operating system.[122] To avoid the risk of being hacked and exposing company and customer information, the business owner should change the password immediately.[123] Second, companies should strive to keep POS software up to date.[124] Developers of these systems constantly upgrade the security features to prevent breaches where hackers have been launching attacks.[125]

Additionally, businesses may find it beneficial to install software on their computer systems to stop hackers from accessing sensitive information.[126] Merchants should be equipped with an industry standard firewall that can stop worms, viruses and other malicious software from gaining access to internal systems.[127] Another standard technique used to prevent hackers from gaining access to important information is the use of antivirus software, which can detect any unwanted and potentially dangerous software residing on the device.[128]

[118] *Id.*
[119] *Id.* (citing BEN KRAFT, ERIC MANNES, & JORDAN MOLDOW, SECURITY RESEARCH OF A SOCIAL PAYMENT APP 5-6 (2014).
[120] Eric Levenson, *Why the Venmo Newsfeed is the Best Social Network Nobody's Talking About,* THE ATLANTIC (Apr. 29, 2014), https://www.theatlantic.com/entertainment/archive/2014/04/why-the-venmo-newsfeed-is-the-best-social-network-nobodys-talking-about/361342/
[121] Held, *supra* note 86.
[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] *Id.*
[126] Held, *supra* note 86.
[127] *Id.*
[128] *Id.*

Finally, experts support the use of two specific controls that can keep unwanted access from disrupting business: restricting access to the point of sale system and preventing employees from accessing the system remotely.[129] These tools can reduce the risk of important information finding its way into the wrong hands.[130] This step highlights the crucial mix of software and human controls that must work in partnership to prevent security breaches. Data breaches may occur again in the future, but with careful planning, the magnitude of the attack can be limited and the speed of the response to the breach can be streamlined.

V. Current Law

As technological developments have blazed new frontiers, the law, at a state, national, and international level, may be behind in developing an adequate framework regarding mobile payment technology. There is no federal law in place to impose a uniform law on all consumers and businesses across the nation.[131] However, many distinct sectors of the economy have their own federal legal regime, which can be further complicated by navigating layers of state laws.[132] For example, the financial and healthcare industries have different rules, in addition to various state laws that impose different rules.[133] This uncertainty and complexity burdens businesses seeking to grow across state lines.[134] The difficultly of navigating an extremely complex patchwork system of laws that may not efficiently promote growth and security.

The current federal laws relevant to mobile payment technology may not sufficiently prioritize safeguarding financial information. However, these laws are very old and do not address the prescient issues facing the industry. Two major pieces of federal regulation are the Truth in Lending Act of 1968 ("TILA") and the Fair Credit Billing Act of 1974 ("FCBA").[135] The TILA protects consumers from fraudulent credit card transactions by requiring that financial institutions provide consumers with a fair and timely resolution of credit billing disputes.[136] The FCBA also limits consumer liability to $50 for any unauthorized or fraudulent charges.[137] These laws place the vast majority of the burden on financial institutions and credit card issuers to ensure the prevention of most attempts at fraud perpetuated by criminals.

[129] *Id.*
[130] *Id.*
[131] Lowry, *supra* note 14, at 370.
[132] *Id.*
[133] *Id.*
[134] *Id.* at 370-71.
[135] *Id.*
[136] Lowry, *supra* note 14.
[137] *Id.*

However, prepaid debit cards do not grant the same protections.[138] While the Federal Deposit Insurance Corporation ("FDIC") does provide regulatory support for consumer accounts associated with credit and debit cards, it does not limit the liability for unauthorized transactions made using stolen prepaid cards.[139] Nonetheless, FDIC insurance may kick in if the prepaid card is linked to an FDIC insured account that fails.[140] In 2014, the Consumer Financial Protection Bureau ("CFPB") proposed new rules for general-purpose prepaid cards that would require companies to limit consumer's losses if a card was lost or stolen.[141] In addition, the FDIC has worked to expand its regulatory reach by stating that these rules, in addition to existing federal laws, apply to mobile payments "when the underlying source of payment is a credit card" as it was concerned that because mobile payment systems do not use the existing payment infrastructure, these systems may be exempt from the laws and regulations of the current infrastructure.[142] Expanding this regulation to include mobile payments systems would place all mobile payment transactions using credit cards under the protection of TILA.[143]

Privacy laws may also have a significant impact on the mobile payments industry. Currently, the relevant laws in place, the Right to Financial Privacy Act of 1978 and the Gramm-Leach-Bliley Act are woefully outdated. These laws have not been updated to reflect the digital age. If regulators fail to update these laws, the many differences pertaining to mobile payments systems compared to traditional credit card systems will become apparent, which could place consumers at risk.

For example, privacy concerns may arise because mobile payment systems often can tag the location of the user, which the user may choose to share on social media. While the design of some systems will prevent users from accidentally sharing this information, the potential still exists for users to accidentally broadcast their location and spending habits to the world. Furthermore, the glut of information that these systems can obtain from their users regarding their purchasing habits will undoubtedly be of interest to retailers and hackers alike. Proper regulation may be key to protecting consumers from the unauthorized dissemination of sensitive information.

As previously mentioned, the myriad of different state laws, which have no overarching federal guidelines, may also hinder the growth of mobile payment systems. For example, digital wallets, such as Apple Pay and Google Wallet, are not considered money transmitters and therefore are not

[138] *Id.* at 368.
[139] Lowry, *supra* note 14.
[140] *Id.*
[141] *Id.*
[142] *Id.* at 378.
[143] *Id.*

subject to state level money transmitter rules.[144] However, while there are state laws in place that require licensure to regulate money transmitters, such as PayPal, the rules vary for all 50 states.[145]

Unfortunately, the federal government has not provided a clear response. Federal regulators have stated that if a mobile payment system uses an existing payment method, such as an Automated Clearing House ("ACH") or electronic funds transfer ("EFT"), the laws and regulations that apply to that form of payment will extend to the mobile version.[146] This includes mobile payments operated and funded by the credit card provider of the user.[147] For these types of transactions, the rules that govern ordinary credit card transactions will continue to apply.[148]

Perhaps the easiest and most efficient solution for federal regulators is to classify the developers of these programs as "regulated financial institutions." Some legal scholars, including Adam Levitin of the Georgetown University Law Center, argue that "[c]ard issuers are covered persons, and Apple is providing a material service in connection with a consumer financial product: a credit card."[149] This theory posits that Apple and Google, among other technology giants that have entered the mobile payment industry are legally now "regulated financial institutions."[150]

At first pass, this theory may seem untenable, but there is some real traction to the argument that many of the largest technology firms in the United States have evolved into financial institutions. Levitin's argument depends on language from the CFPB that gives it regulatory authority over any institution that participates in "designing, operating, or maintaining [a] consumer financial product or service."[151] The key difference between former Apple products, which facilitated mobile payments, and its new proprietary software, Apple Pay, is that the latter entails the operation and maintenance of a mobile payment system.

While new and existing businesses may protest additional regulation, it would not defy industry precedent, as banking has long been one of the most highly regulated trades in the United States.[152] Included in the

[144] Lowry, *supra* note 14, at 376.
[145] *Id.* at 369.
[146] *Id.* at 377.
[147] *Id.*
[148] *Id.*
[149] Lowry, *supra* note 14, at 380 (quoting Adam Levitin, *Apple Pay and the CFPB*, CREDIT SLIPS (Sept. 10, 2014, 10:56 PM), http://creditslips.org/creditslips/2014/09/apple-pay-and-the-cfpb.html).
[150] *Id.*
[151] *Id.*
[152] *Id.* at 355-56.

regulatory framework are a multitude of state agencies and a wide variety of federal regulators.[153] The most prominent among these include the Federal Reserve, FDIC, Office of the Comptroller of the Currency ("OCC"), Securities and Exchange Commission ("SEC"), and the Commodity Futures Trading Commission ("CFTC").[154] Additionally, after the financial crisis in 2008, Congress created the CFPB with the Dodd-Frank Act.[155] The main purpose of the CFPB is the protection of the financial interests of consumers.[156]

The Dodd-Frank Act also included the controversial Durbin Amendment that increased regulation on banks, which some argue has hampered growth in the mobile payment industry.[157] The Durbin Amendment has affected the mobile payment industry in ways that were likely not intended and perhaps not envisioned at the time of the law's passage, when mobile payments were still in their infancy.[158] The legislation has burdened the mobile payment industry by redistributing costs throughout the banking system.[159] Rather than enacted laws the place burdens on the mobile payment sector, industry insiders believe that "financial institutions must be the catalysts that drive the growth of mobile payments."[160] Additionally, the legislation requires a twenty-one cent interchange fee per transaction, which has had unintended anticompetitive consequences that have prevented new and smaller competitors from entering the market.[161]

The stated purpose of the Amendment was to "help small businesses, merchants, and consumers by providing relief from high interchange fees for debit card transactions."[162] In 2010, the fees averaged forty-four cents per debit card transaction processed by a merchant.[163] Therefore, while the twenty-one cent cap has been beneficial to consumers in certain aspects, it has switched from imposing a ceiling on the costs of those transactions, to imposing a floor for transaction costs below which businesses cannot go.[164] Armed with new technology, firms are finding it more difficult to justify

[153] Lowry*, supra* note 14, at 356.
[154] *Id.*
[155] *Id.*
[156] *Id.*
[157] Reinisch, *supra* note 17, at 137.
[158] *Id.*
[159] *Id.*
[160] *Id.*
[161] *Id.*
[162] *Id.*(quoting M. Pierce Sandwith, Note, *Debit Card Interchange Fees and the Durbin Amendment's Small Bank Exemption*, 16 N.C. BANKING INST. 223, 232-33 (2012) (quoting 156 Cong. Rec. S3695 (daily ed. May 13, 2010) (statement of Sen. Richard Durbin))).
[163] *Id.*
[164] *See id.* at 124.

innovating with this artificial price barrier.[165] As per transaction costs continue to dwindle as new technology comes online, it will be crucial for legislators to continue to monitor the viability of fixed-price regulations to refrain from impeding the market.

It is possible that the myriad of different laws and regulations, as well as their applicability to current technology, has stifled the innovation of mobile payment technology. With uneven legislation and an unknown direction for regulation, firms, and individuals may be hesitant to risk investing in resources to develop new technology. Regulators must be sensitive to the rapidly changing technological capabilities of mobile payment systems, while also protecting unwary consumers and the integrity of financial institutions. In a period of uncertain politics and rapid dynamic change in the economy, regulators must be forward-looking and thoughtful, while continuing to consider the needs of their constituents.

VI. PROPOSED SOLUTIONS

The significant issues with the legal framework surrounding the mobile payment industry have attracted a myriad of different regulatory proposals. However, the correct mix of regulation for this rapidly evolving industry has proven difficult to enact. Prolonged debates in Congress and various statehouses over relatively inconsequential matters have delayed the necessary large-scale protections that consumers need. Security and transparency are the keys to the success of the mobile payments industry. Regardless, unless there is a fruitful partnership between Silicon Valley and Washington, D.C., mobile payment systems may not achieve their full potential.

One proposed solution includes creating an exception to the interchange-fee ceiling for mobile payments processed by certain companies and issuers.[166] The model for this proposal is the exemption cap on interchange fees for banks with less than $10 billion in assets.[167] This could reverse the allegedly deleterious impact of the Durbin Amendment on the industry.[168] That legislation has had the effect of curtailing innovation and new market entrants by redistributing wealth, which impairs the incentives to innovate and be the first mover in the industry.[169]

Another proposed regulatory framework to some of the legislative impediments in the mobile payment industry is further utilization of HCE technology. This technology has the potential to create a greater level of

[165] *Id.*
[166] Reinisch, *supra* note 17, at 151.
[167] *Id.*
[168] *Id.* at 152.
[169] *Id.* at 151.

security that will further strengthen the relationships between consumers and their financial institutions.[170] In this system, the physical Smartphone is the key to solving one of the major issues facing the widespread adoption of mobile payments - user authentication.[171] HCE technology would enable further encryption of consumer data, [172] which in turn could encourage consumer confidence and adoption of mobile payment technology.

HCE technology functions by creating an exact replica of the card using only software.[173] This may be more secure since the actual card profile does not need to be stored on the phone on a specialty chip, called a Secure Element.[174] As an added bonus, banks can use location services on the phone to attempt to detect fraudulent transactions.[175] This includes utilizing features such as "proximity to Wi-Fi locations, 3G location, GPS data, and the number and type of applications on the device to build a unique profile for each phone."[176]

This technology will not necessarily protect against credit fraud, but it has the potential to help detect and determine the likelihood of a fraudulent transaction.[177] For example, if a transaction occurs in an unusual place at a time of the day when and where that consumer does not typically make financial transactions, an algorithm in the system might tip-off the issuer to a potential fraudulent transaction.[178] The key to the widespread adoption of this system would be the successful development of an algorithm that would catch enough fraudsters to gain the trust of the public, while simultaneously protecting the privacy of individuals and not annoying users with incessant, overly sensitive fraud alerts.

Furthermore, mobile payment technology has the potential to help streamline the in-store consumer experience. As an example, Sam's Club recently released a new app, Scan & Go, which allows users to scan items while shopping and place them in their cart.[179] Once the customer finishes shopping, the app processes payment and the user leaves the store after an employee at the exit spot checks carts to ensure there has been no theft.[180] In

[170] *Id.*
[171] Reinisch, *supra* note 17, at 151.
[172] *Id.*
[173] *Id.*
[174] *Id.*
[175] *Id.*
[176] Moulds, *supra* note 80.
[177] *Id.*
[178] *Id.*
[179] Kate Fitzgerald, *Could Sam's Cub's new app spell the end of big-box checkout lines?*, PAYMENT SOURCE (Nov. 21, 2016), https://www.paymentssource.com/news/ could-sams-clubs-new-app-spell-the-end-of-big-box-checkout-lines.
[180] *Id.*

this system, the consumer barely speaks to or interacts with a human being for the entire shopping experience.[181] While this technology remains unproven, it shows another instance in which regulation may be necessary to protect consumer identity and promote business efficiency.

Similarly, online retail giant Amazon recently developed and built a concept grocery store that uses a similar format, where items are added to the "shopping cart" of the consumer after removal from the shelves, and then charged to the user's account when the user leaves the store.[182] While this new format for the consumer retail experience may involve many other areas of regulation, ensuring the security of the mobile application and maintaining the confidence of consumers are crucial to supporting the development of this new technology and retail model.

Finally, policymakers should consider the three mechanisms that industry experts believe have significant potential to advance security in the mobile payment industry. These include tokenization, device-specific cryptograms, and two-factor authentication.[183] Tokenization works by sending a randomly generated token to the point of sale when a consumer makes a purchase.[184] This is different from swipe or chip transactions with a standard credit card because the mobile wallet does not transmit the card's primary account number.[185] This prevents hackers and thieves from being able to steal the sensitive information while it is in transit.[186]

The industry association for mobile payments, ISACA, prefers tokenization technology and considers it the "security solution that is pushing mobile payments ahead of card payments in consumer sensitive financial information protection in the continuous race to stay ahead of hackers and other threats."[187] Tokens only work for transactions that match specific criteria for the exact period of time, specific retailer, and certain monetary value.[188] Therefore, the transaction processes only after the consumer's bank

[181] See *id.*

[182] Laura Stevens, *Amazon Working on Several Grocery Store-Formats, Could Open More Than 2,000 Locations,* THE WALL STREET JOURNAL (Dec. 5, 2016), http://www.wsj.com/articles/amazon-grocery-store-concept-to-open-in-seattle-in-early-2017-1480959119.

[183] *ISACA Challenges Mobile Payment Security Perceptions,* ISACA (July 20, 2016), http://www.isaca.org/About-ISACA/Press-room/News-Releases/2016/Pages/ISACA-Challenges-Mobile-Payment-Security-Perceptions.aspx [hereinafter *ISACA*].

[184] *Id.*

[185] *Id.*

[186] *Id.*

[187] *Id.*

[188] ISACA, *supra* note 183.

and authorized entities can securely map tokens back to the original payment card data.[189]

Another potential security solution for mobile payment technology is the use of device specific cryptograms. These systems ensure that the payment originated from the correct source–that cardholder's device.[190] If a hacker can obtain the transaction data, "the cryptogram that is sent to the POS terminal with the token is unable to be used on another mobile device."[191] This stops the transaction from being processed and causes the stolen data to be "un-forgeable and useless," which would protect the consumer and retailer from theft.[192]

The final proposed solution is two-factor authentication, which would help to prevent fraud by "utilizing two independent mechanisms for authentication."[193] Many of the security features utilized by two-factor authentication are already present in the hardware and software on current mobile devices.[194] These features include passwords, which are made of personal information or random numbers and letters, a physical device, such as a credit card or a phone that must be used to complete the transaction, and a biometric component such as a fingerprint, voiceprint or facial recognition.[195] A system using two-factor authentication combines any two of these options in order to safeguard the information of the consumer.[196] ISACA has found, in an industry survey, that two-factor authentication would be the easiest to roll out and gain widespread adoption.[197] That survey found that respondents were far less keen to adopt technology such as the use of limited duration codes and phone-based security applications.[198]

ISACA notes that the most important action that consumers can take to improve the security of their mobile payments is the use of two-factor authentication.[199] While a combination of these three technological options would provide the greatest level of financial security for consumers, the widespread use or implementation of any one of the three would provide sufficient security to consumers and would benefit growth of the industry by providing clear guidance and concrete rule in which to operate.

[189] *Id.*
[190] *Id.*
[191] *Id.*
[192] *Id.*
[193] ISACA, *supra* note 183.
[194] *Id.*
[195] *Id.*
[196] *Id.*
[197] *ISACA Survey*, *supra* note 12.
[198] *Id.*
[199] *Id.*

VII. CONCLUSION

As the mobile payment industry continues to alter the landscape of the credit and debit card industry, it is crucial that legislators work closely with innovators and technology giants to provide the greatest benefit to banks, consumers, and retailers. The seismic shift towards mobile payments and away from physical plastic credit cards and cash is likely the greatest shift since the invention and widespread adoption of the credit card many decades ago. Coupled with the blinding speed of technological innovation and the malicious intentions of devious hackers, it is critical that laws help address the most pertinent issues, while fostering an environment that is receptive to dynamic change.

Merchants must also embrace this new technology as it continues to transform the shopping experience of consumers. Forward thinking retailers will reap the rewards of increased security measures, which could lower fraud costs.[200] If the legal system is able to help developers understand and efficiently navigate the very real security risks to consumers, some potential issues may be cut-off before the adverse consequences materialize. The rapid changes in the mobile payment space are fascinating developments, and should complement optimal regulation to ensure the long-term stability of the technology. The legal industry cannot sit idly by, for proper regulation is the key to reducing transactions costs, limiting fraud, and ensuring developers have the proper incentives to pursue innovation.

[200] *ISACA*, *supra* note 183.