HOW APPLE PAY COINCIDES WITH THE CONSUMER FINANCIAL PROTECTION ACT: WILL APPLE BECOME A REGULATED ENTITY?

Jessica M. Gray*

I. INTRODUCTION

In today's world, it is almost a guarantee that from the time a person wakes up in the morning until the time a person goes to bed, he or she will see numerous people using their smartphones throughout the day.[1] Of all the smartphones captivating the public, Apple's iPhone has proven to be the most desirable.[2] When the original iPhone launched on June 29, 2007, people waited in line for hours in anticipation of something that had only been imagined in the mind of

* J.D. Candidate, Suffolk University Law School, 2016.

[1] *See* Aaron Smith, *U.S. Smartphone Use in 2015*, PEW RESEARCH CENTER (Apr. 1, 2015), *archived at* http://perma.cc/534U-DSZV (reporting that "64 percent of Americans now own a smartphone of some kind, up from 35 percent in the spring of 2011").

[2] *See* Mikey Campbell, *Apple Continues to Gain Ground in US Smartphone Market as Android Shrinks*, APPLEINSIDER (Aug. 7, 2015), *archived at* http://perma.cc/7JZD-QGBD (discussing Apple's dominance in the U.S. smartphone market). Apple's "iPhone grew its share of the U.S. market to 44.1 percent in June" 2015, selling 47.5 million iPhones over the June quarter, a record-breaking performance. *Id.*

 ISSN 1536-7983.

the late Steve Jobs, Apple's CEO at the time.[3] For the next seven years, Apple constantly challenged itself by inventing new iPhones that trumped the features of the previous generation of iPhones.[4] However, it was not until October of 2014 that Apple introduced a feature of its newest iPhone that has the potential to not only dramatically affect its consumers, but also the company itself—Apple Pay.[5]

The digital wallet represents a future where consumers will no longer have to dig through purses or physical wallets in search of plastic credit cards or cash, but where they can simply scan or swipe their device at the register.[6] Apple Pay, available only on the iPhone 6, the iPhone 6 Plus, and the Apple Watch, turns the device into a digital wallet, allowing a person to use the feature to pay at one of 220,000 contactless payment locations across the nation, including McDonalds, Walgreens, and Macy's.[7] In 2011, Google attempted to launch its form of the digital wallet, but it ultimately failed to succeed in the market.[8] Despite past flops of the digital wallet, Apple Pay is the first to have a momentous global impact, particularly because Apple, as a company, has already successfully shown its ability to in-

[3] *See* Rene Ritchie, *History of iPhone: Apple Reinvents the Phone*, IMORE (Aug. 31, 2015), *archived at* http://perma.cc/D7QR-48EE (describing the history of the iPhone and its introduction to the public).

[4] *See* Jessica Durando, *iPhone 6, iPhone 6 Plus: See All Generations of iPhones*, USA TODAY (Sept. 9, 2014), *archived at* http://perma.cc/44T5-5ZF2 (recapping the iPhone's innovations since 2007).

[5] *See* Kevin Cirilli & Julian Hattem, *Did Apple Just Become a Big Bank?*, THE HILL (Sept. 14, 2014), *archived at* http://perma.cc/ARW4-AYYV (analyzing Apple's use of mobile banking through Apple Pay and whether this may lead to oversight from federal regulators). Apple Pay's transition into the world of e-commerce could convince millions of customers and stores to switch out the plastic credit cards for the chip in their phone, forcing lawmakers and regulators to race to catch up with the quick technological advancement. *Id.*

[6] *See* Edward Castronova & Joshua A.T. Fairfield, *The Digital Wallet Revolution*, N.Y. TIMES (Sept. 10, 2014), *archived at* http://perma.cc/82LX-RJJE (evaluating the impact of the digital wallet on society, including advantages and concerns). The digital wallet may set forth a new era of ease and convenience, but it also may create challenges for governments around the world. *Id.*

[7] *See* Sebastian Anthony, *Apple Unveils Apple Pay, a Digital Wallet for Your iPhone 6 and Apple Watch*, EXTREMETECH (Sept. 16, 2014), *archived at* http://perma.cc/WGA6-RJFQ (outlining how Apple Pay works and which companies it has partnered with).

[8] *See* Edward C. Baig, *Apple Pay May Be Game-Changing Play*, USA TODAY (Oct. 5, 2014), *archived at* http://perma.cc/KJN3-F2D7 (highlighting previous attempts of companies to create a digital wallet that would attract customers).

crease consumer fanaticism over its products.[9] During Apple's quarterly conference for the first quarter of 2015, Apple CEO Tim Cook described the rapid growth in Apple Pay since it was unveiled.[10] Since retailers have eagerly adopted Apple Pay, the payment application "now accounts for two out of every three dollars processed through contactless payment systems."[11] However, a feeling of uncertainty over mobile payment systems is still abundant among customers due to the significant increase in security attacks and data breaches of major companies like Facebook, Twitter, Microsoft, and even Apple itself.[12]

The introduction of Apple Pay may embody the future of mobile financial services for consumers, but Apple may have simultaneously and unknowingly entered a realm of federal regulation.[13] This Note will argue that Apple is a "service provider" under the Consumer Financial Protection Act, and thus it is subject to financial regula-

---

[9] *See* John Heggestuen, *6 Reasons Why Apple Pay Will Catch On And Walmart Will Have To Accept It*, BUSINESS INSIDER (Oct. 27, 2014), *archived at* http://perma.cc/8WFD-7N5N (illustrating how Apple's influence on consumers may trigger Apple Pay's future success).

[10] *See* AppleInsider Staff, *Tim Cook Calls 2015 the 'Year of Apple Pay' as Service Takes Over Contactless Payments Market*, APPLEINSIDER (Jan. 27, 2015), *archived at* http://perma.cc/U86T-C9V7 (outlining Tim Cook's speech at Apple's first quarterly conference of 2015). Cook stated, "We are more confident than ever that 2015 will be the year of Apple Pay." *Id.*

[11] *See id.* (highlighting the rapid success of Apple Pay largely due to retailers updating their point-of-sale terminals so that they are compatible with Apple Pay).

[12] *See* Simon Godfrey, *2014 – The Year of the Hacker?*,TECHRADAR (Feb. 17, 2014), *archived at* http://perma.cc/SCD5-S8GM (underlining the concerns of the increase in cyber attacks in 2013 and the need to raise awareness); *see also* Elizabeth Weise, *Will Apple Pay Be Safer Than Credit Cards?*, USATODAY (Sept. 10, 2014), *archived at* http://perma.cc/E8EG-7VVR (discussing Apple Pay's security measures, including the use of a PIN number and fingerprint, rather than the magnetic strip of a credit card); Jim Finkle & Andrew Hay, *Apple iOS Bug Makes Most Devices Vulnerable to Attack, Researchers Say*, THE HUFFINGTON POST (Nov. 10, 2014), *archived at* http://perma.cc/N3XK-4KPY (reporting on Cybersecurity firm FireEye's findings that a bug in Apple's iOS operating system makes iPhones and iPads vulnerable to hackers by tricking users into installing dangerous applications with tainted text messages, emails, and web links). This type of hacking method allows hackers to steal sensitive data including banking and email login credentials. *Id.*

[13] *See* Cirilli & Hattem, *supra* note 5 (exploring whether or not Apple Pay has transformed Apple into a company that can now be federally regulated as a financial institution).

tions.[14] This Note will also discuss the role of the Consumer Financial Protection Bureau and its responsibility in upholding the legal implications of the Consumer Financial Protection Act. This Note will then consider what it will mean for Apple to be regulated under this law and subsequently tie in how Apple may potentially be affected by Massachusetts General Laws chapter 93A. The analysis will provide hypotheticals of possible security issues with Apple Pay and how consumers can legally respond to such breaches, both federally and in Massachusetts. This Note will ultimately hypothesize Apple's future, if it becomes federally regulated under the Consumer Financial Protection Act, and how this future could consequently benefit consumers.

II. HISTORY

A. The Consumer Financial Protection Act of 2010

In 2007, the United States was beginning to enter the biggest financial storm since the Great Depression.[15] While jobs were lost and home values plummeted, lenders capitalized on the dire situation by luring tens of millions of American families into unaffordable loans by false promises of low payments.[16] In June 2009, President Obama urged Congress to address the lack of consumer protection by creating a new financial institution that would center its attention on protecting people from "unfair, deceptive, and abusive financial practices."[17] In July 2010, Congress passed the Dodd-Frank Wall Street

[14] *See* 12 U.S.C. § 5481 (2010) (defining terms under the Consumer Financial Protection Act).

[15] *See Creating the Consumer Bureau*, CONSUMER FINANCIAL PROTECTION BUREAU, *archived at* http://perma.cc/XM8R-DN92 (describing the historical circumstances that led to the establishment of the Dodd-Frank Wall Street Reform and Consumer Protection Act).

[16] *See id.* (outlining the impact of deceptive business practices by lenders on borrowers). Many lenders took advantage of gaps in the consumer protection system by selling mortgages that people could not afford and giving misleading promises of low payments. *Id.*

[17] *See id.* (highlighting the intent behind creating a new financial agency that would deal directly with consumers, rather than on banks or financial companies).

> This new agency would heighten government accountability by consolidating in one place responsibilities that had been scattered across government. The agency would also have responsibility for supervision and enforcement with respect to the laws over

Reform and Consumer Protection Act, which, in turn, created the Consumer Financial Protection Bureau to protect American consumers in the market for consumer financial products and services.[18] The Consumer Financial Protection Bureau, headed by an appointed director, has the power to "administer, enforce, and otherwise implement federal consumer financial laws."[19]

Under the Consumer Financial Protection Act, the Bureau has authority over numerous consumer financial products and services, including mortgages, credit cards, and money transmissions.[20] The original version of the bill defined a service provider as those persons who have "direct interaction with a consumer, or facilitate, or make easier, the design or operation of a transaction."[21] The revised lan-

> providers of consumer financial products and services that escaped regular Federal oversight. This agency would protect families from unfair, deceptive, and abusive financial practices. The President urged Congress to give the consumer agency the same accountability and independence that the other banking agencies have and sufficient funding so it could ensure that powerful financial companies would comply with consumer laws.

Id.

[18] *See id.* (stating the establishment of the Consumer Protection Act and the purpose of the Consumer Protection Bureau, which ultimately consolidates most federal consumer financial protection authority in one place); *see also* 12 U.S.C. § 5301 (2010) (providing the definitions used within the Wall Street Reform and Consumer Protection Act); *Consumer Finance*, FEDERAL TRADE COMMISSION, *archived at* http://perma.cc/A5M7-9RFQ (summarizing the responsibilities of the Consumer Protection Bureau and its relationship to the Federal Trade Commission).

[19] *See* 12 U.S.C. § 5511 (2010) (outlining the purpose, objective, and functions of the Consumer Financial Protection Bureau); *see also* 12 U.S.C. § 5514 (2010) (defining who is covered under the act and subject to regulation by the Consumer Financial Protection Bureau); *About us*, CONSUMER FINANCIAL PROTECTION BUREAU (Aug. 26, 2014), *archived at* http://perma.cc/RVX9-CJDN (explaining the mission, core functions, and structure of the Bureau); Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 tit. 10 (2010) (outlining the main provisions of the Consumer Financial Protection Act, including the role of the Bureau).

[20] *See* 12 U.S.C. § 5481(15) (defining a "financial product or service"); *see also* Dodd-Frank Wall Street Reform and Consumer Protection Act §1002(15) (describing mortgages, credit cards, and money transmissions); DAVID H. CARPENTER, CONG. RESEARCH SERV., THE CONSUMER FINANCIAL PROTECTION BUREAU (CFPB): A LEGAL ANALYSIS 13 (2014) (discussing overview of the bureau's authority).

[21] *See* Valerie L. Hletko & Sarah E. Hager, *Which One of Us Is the Service Provider? The Dodd-Frank Act's Infinite Loop of Oversight*, EMERGING ISSUES ANALYSIS (Aug. 2013), *archived at* http://perma.cc/5ELP-3BAJ (exploring the issue of cate-

guage now states that a service provider refers to "any person that provides a material service to a covered person in connection with the offering or provision by such covered person of a consumer financial product or service."[22] The definition includes providers that design, operate, or maintain the product or service, as well as those that process transactions relating to the product or service.[23] Although historically the Consumer Financial Protection Act has dealt with the traditional financial institution of banks, the technological advances of mobile banking through a digital wallet have raised new questions concerning what federal or state banking and financial services laws and regulations would govern these mobile payment services.[24] Various interpretations of the statutory language leave the door open for litigation surrounding the definition of a service provider and the intent behind the legislature in how broadly to apply the definition.[25]

B. Relationship between the Federal Law and Massachusetts General Law chapter 93A

The Consumer Financial Protection Act does not preempt state consumer financial protection laws so long as the state laws do not conflict with federal laws or regulations.[26] Further, state statutes that afford consumers greater protection than federal laws do not conflict with federal laws.[27] The attorney general of any state can bring a

gorizing who qualifies as a service provider through an analysis of the Act's statutory language and legislative history) (quoting 16 H.R. 4173, 111th Cong.§ 40002(35)(A) (2009).

[22] *See* 12 U.S.C. § 5481(26) (defining "service provider" under the Consumer Financial Protection Act).

[23] *See id.* (elaborating on the particulars of the "service provider" definition).

[24] *See* 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, 455-56 (2013) (exploring the potential need for future laws and regulations that will apply to mobile banking).

[25] *See* Hletko & Hager, *supra* note 21 (interpreting the line one would have to cross in order to be considered a service provider versus a service receiver).

[26] *See* 12 U.S.C. § 5551(a)(1)-(2) (2015) (stating the Consumer Financial Protection Act's relationship to state law).

[27] *See* 12 U.S.C. § 5551(a)(2) (explaining balance with state authority).

> For purposes of this subsection, a statute, regulation, order, or interpretation in effect in any State is not inconsistent with the provisions of this title if the protection that such statute, regulation, order or interpretation affords to consumers is greater than the protection provided under this title.

civil action on behalf of a resident of the state or in the form of a class action in order to enforce provisions and remedies under the federal law.[28] In Massachusetts, the consumer protection law is known as Massachusetts General Law chapter 93A.[29] The Attorney General may investigate and take legal action against businesses that participate in unfair or deceptive conduct, and prosecute a consumer protection case in the public interest, as well as in a private lawsuit.[30] The Massachusetts law is an attractive outlet for wronged parties to seek justice under because a person may recover double or treble damages, as well as attorneys' fees and costs.[31] Under the federal Consumer Financial Protection Act, courts or the Bureau may award any appropriate legal or equitable relief.[32] However, exemplary or punitive damages are not to be awarded under the Act.[33] Essentially, if the Consumer Financial Protection Bureau opted not to pursue litigation over a particular matter, the Massachusetts Attorney General could bring a civil action under both the federal Consumer Financial Protection Act, as well as under 93A, and potentially recover a greater monetary sum.[34]

Id.

[28] *See* 12 U.S.C. § 5552(a)(1) (2015) (stating that the attorney general of any State may bring a civil action in the name of that State to enforce the provisions of the Consumer Financial Protection Act).

[29] *See* MASS. GEN. LAWS ch. 93A (2015) (describing the application, procedures, and potential liability under the Massachusetts statute that has the purpose of protecting consumers from unfair and deceptive business practices).

[30] *See Taking Action: The Consumer Protection Law*, MASS.GOV, *archived at* http://perma.cc/Q6HL-FZ8W (explaining what is covered in Massachusetts General Law chapter 93A and providing an example of how a demand letter should be executed). A consumer begins a c. 93A action by first sending a demand letter to the business, which has the purpose of putting the business on notice, potentially convincing the business to settle the matter outside of court, and lastly the letter acts as a formal control of money damages the consumer may recover in court. *Id.*

[31] *See* MASS. GEN. LAWS 93A § 9(1) (2015) (stating who is entitled to bring an action under this chapter, the requirement of a written demand for relief, and the potential amount of damages available to the claimant).

[32] *See* 12 U.S.C. § 5565(a)(1)-(2) (2015) (stating that the court or the Bureau has jurisdiction to grant relief with respect to a violation of federal consumer financial law).

[33] *See* 12 U.S.C. § 5565(a)(3) (stating that relief under this § 5565 never includes exemplary or punitive damages).

[34] *See* Ashley L. Taylor, Jr. et. al., *The Consumer Financial Protection Bureau and the State Attorneys General: A Force Multiplier in Consumer Protection Matters*, BLOOMBERG LAW REPORTS (May 25, 2011), *archived at* http://perma.cc/ECY8-TXBR (outlining the purpose, objectives, and organization of the Consumer Finan-

C. Recent Surge in Data Breaches

In 2013, United States consumers were the victims of a dramatic increase in the number of security attacks and data breaches.[35] Between July and October 2013, personal information from more than 1.1 million debit and credit cards was stolen from Neiman Marcus stores.[36] In January 2014, Snapchat, a photo and video-sharing application, suffered a data breach in which usernames and partial phone numbers of 4.6 million subscribers were exposed.[37] As different forms of electronic communication become more prevalent in today's world, especially e-commerce and e-banking, security protocol for various organizations, including TJX, Hannaford, and Sony Playstation, have come under intense scrutiny.[38] In a lawsuit filed by Massachusetts Attorney General Martha Coakley, several popular Boston bars and restaurants were forced to pay $110,000 under settlement due to a data breach that put the payment card information of tens of thousands of consumers at risk.[39] Under the terms of the set-

cial Protection Act of 2010). The state Attorney General or appropriate state regulator may bring a civil action, in the name of the state, to enforce provisions of the federal Act, except with respect to a national bank or federal savings association. *Id.*

[35] *See* Godfrey, *supra* note 12 (discussing the increased hacking attacks that are cause for concern for consumers, as well as security professionals). Facebook, Twitter, Microsoft and Apple all suffered security attacks in 2013. *Id.*

[36] *See Data Breach Lawsuit Legal News and Information*, LAWYERSANDSETTLEMENTS.com (Oct. 24, 2014), *archived at* http://perma.cc/B8JF-KM72 (recapping the most recent and damaging data breach lawsuits).

[37] *See id.* (recounting Snapchat's recent data breach in 2014); *see also* Brian Fung, *A Snapchat Security Breach Affects 4.6 Million Users. Did Snapchat Drag its Feet on a Fix?*, THE WASHINGTON POST (Jan. 1, 2014), *archived at* http://perma.cc/ZUV7-J5HY (detailing a security lapse in the Snapchat application which led to a breach of sensitive information).

[38] *See* Timothy H. Madden, *Data Breach Class Action Litigation – A Tough Road for Plaintiffs*, 55 BOS. BAR J. 27, 31 (2011) (examining the increase in data breach cases and the difficulty of plaintiffs to succeed in court due to failure of demonstrating they suffered actual harm). Plaintiffs have to demonstrate that they have suffered actual harm, such as fraudulent use of their financial information, in order for courts to allow their claims to proceed through the earliest stages of litigation. *Id.*

[39] *See* Press Release, Mass.gov, Major Boston Restaurant Group That Failed to Secure Personal Data to Pay $110,000 Under Settlement with AG Coakley (Mar. 28, 2011) (on file with author) (summarizing the 2011 judgment requiring the Briar

tlement, all of the restaurants were required to create a stronger security system, including a security password management system.[40] Although this case proved to be successful for Massachusetts plaintiffs, its victory is not representative of the few other data-breach related cases in the state.[41]

Many data breach plaintiffs often assert causes of action under state consumer protection statutes, which generally proscribe deceptive and unfair business practices, as described in Massachusetts General Law chapter 93A.[42] The First Circuit in *In re TJX Companies Retail Security Breach Litigation*[43] held that a court could find that the company's lack of security measures constitutes an unfair practice because such conduct is systematically reckless, "aggravated by [a] failure to give prompt notice when lapses were discovered internally, and causing very widespread and serious harm to other companies and to innumerable consumers."[44] Data breach victims may also seek to bring actions under other federal statutes, including sections of the Electronic Communications Privacy Act and the Stored Communications Act.[45] Although historically the litigation

Group to pay civil penalties due to a failed security system that compromised payment information of numerous customers).

[40] *See id.* (elaborating on the settlement stipulations of the Briar Group). All restaurants in the Briar Group Chain were required to implement data security measures to comply with Payment Card Industry Data Security Standards, including implementation, maintenance, and adherence to a Written Information Security Program. *Id.*

[41] *See* Madden, *supra* note 38 (highlighting the lack of success for plaintiffs in data breach cases in the Massachusetts courts).

[42] *See* MASS. GEN. LAWS ch. 93A, § 2 (2015) (stating that "unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful"); *see also* Douglas H. Meal, *Private Data Security Breach Litigation in the United States*, *in* PRIVACY AND SURVEILLANCE LEGAL ISSUES 101, 102-04 (Thompson Reuters/Aspatore, 2014) (illustrating how data security breaches are litigated, including potential litigants, form of damages, procedural issues, and asserted causes of action).

[43] *See* 564 F.3d 489, 491 (1st Cir. 2010) (outlining a case in which banks issuing credit and debit cards to customers had their credit and debit card information stolen from a discount store operator's computers). The banks brought an action against discount store operator and bank serving as "processing bank" for discount store operator's transactions alleging various claims, including violation of Massachusetts's unfair or deceptive practices law. *Id.* at 491-92.

[44] *See id.* at 496 (addressing a factor that constitutes conduct that would be in violation of chapter 93A under the Federal Trade Commission's interpretation).

[45] *See* Meal, *supra* note 42, at 114-15 (listing the federal statutes that data breach plaintiffs may occasionally bring actions under, though not as frequently). Actions

surrounding data breaches has not intersected with the Consumer Financial Protection Act, the technological development of mobile payment and the digital wallet may in fact spark cases that will require a fresh analysis of how these progressive companies should be labeled.[46]

D. Apple's Interaction with the Law

With every new feature or advancement that Apple attempts to set forth in its latest generation of the iPhone, the more concern about the security of its mobile devices grows.[47] In 2011, many privacy advocates and government officials expressed concerns over the ability of mobile devices, like Apple's iPhone, to retain locational data.[48] Apple admitted to encountering an issue with its software that allowed iPhones to store locational data for an excessive amount of time.[49] Although this appeared to be a significant security issue, no one presented evidence that he or she was negatively affected by the saved locational data, thus preventing the opportunity for successful litigation.[50]

Contrary to Apple's locational data bug, which ultimately did not prove to be harmful to consumers or brand the company as en-

are infrequently brought under the Electronic Communications Privacy Act, commonly known as the Wiretap Act, because "a plaintiff must allege that the defendant engaged in the intentional interception, disclosure, or use of data or communications" in violation of the Act. *Id.* at 115. Claims for violation of the Stored Communications Act, which bar providers of specific communication services from revealing private communications to third parties, have also not proved to be the most successful outlet for relief. *Id.*

[46] *See* Meal, *supra* note 42, at 114-15 (analyzing the causes of action and federal statutes that consumers look to after suffering a data security breach).

[47] *See* Adam Thierer, *Apple, The iPhone and a Locational Privacy Techno-Panic*, FORBES (May 1, 2011), *archived at* http://perma.cc/YF4Z-F2QW (discussing concerns raised about Apple iPhones and Google Android-based smart phones retaining locational information). The locational data refers to a "tracking" feature in the device that collects data about user whereabouts. *Id.*

[48] *See id.* (stating the outrage of officials and privacy advocates that locational data retention is a major violation of privacy). A struggle exists concerning the need to adhere to consumer concerns over privacy and the desire for technological innovation. *Id*.

[49] *See id.* (affirming Apple's admittance that it experienced a bug in its software that allowed iPhones to store locational data for a long period of time).

[50] *See id.* (expressing that no one appeared to be negatively affected by the saving of locational data for an extended period of time).

gaging in unfair business practices, in 2014 Apple Inc. was in violation of the Federal Trade Commission Act.[51] Apple billed consumers for millions of dollars of charges incurred by children who bought mobile apps without their parents' consent.[52] The Federal Trade Commission recognizes that the mobile payment arena is quickly advancing, requiring consumer protection enforcement to be a top priority.[53] Apple and other companies, striving for a similar kind of cyber advancement in the mobile world, are forced to weigh the benefits and ill effects of entering a realm that could potentially break down technological barriers and simultaneously sacrifice the protection of its consumers.[54]

Apple has most recently come under public scrutiny due to the hacking of nude photos of dozens of female celebrities.[55] Although traditionally data breach lawsuits are dismissed or settled out of court, this most recent event could allow for litigation that will require Apple to appear in court, and thus it will lead to the establishment of guidelines or standards for how tech companies must conduct

[51] *See* Press Release, Federal Trade Commission, Apple Inc. Will Provide Full Consumer Refunds of At Least $32.5 Million to Settle FTC Complaint It Charged for Kids' In-App Purchases Without Parental Consent, (Jan. 15, 2014) (on file with author) (discussing Apple's settlement with the Federal Trade Commission due to consumers harmed by Apple's unfair billing). The settlement required Apple to modify its billing practices to ensure that Apple obtains the express, informed consent of consumers purchasing mobile apps prior to billing them. *Id.*

[52] *See id.* (describing the Federal Trade Commission's complaint, which alleged that Apple failed to tell parents that by entering a password they "were approving a single in-app purchase and also 15 minutes of additional unlimited purchases their children could make without further action by the parent").

[53] *See id.* (detailing how expanding mobile technology is and must continue to be a main area of focus for the Federal Trade Commission).

[54] *See* Issie Lapowsky, *We'd All Benefit if Celebs Sue Apple Over the Photo Hack*, WIRED (Sept. 2014), *archived at* http://perma.cc/8WFB-73J6 (analyzing the potential for a negative public reaction if Apple were to create stricter log in credentials and sacrifice the speed and fluidity of technological innovation). As Professor Fred Cate said "Whenever a company raises the security bar, the public hates it. So they're [Apple] sort of in a Catch-22. We hate them when they make us use top security, but we hate them when they lose our data." *Id.*

[55] *See id.* (describing Apple's position in the celebrity hacking scandal and the potential legal consequences if those hacked celebrities choose to pursue litigation). Apple denied that there was a breach of any Apple systems, including iCloud and FindMyiPhone, but rather stated that the incident was "a very targeted attack on user names, passwords and security questions, a practice that has become all too common on the Internet." *Id.*

their business.[56] The Federal Trade Commission may examine the security measures embraced by Apple and determine whether or not they are substantial enough to provide consumers with reasonable security protection.[57] Establishing Apple's role in security attacks will require an analysis, by the correct agency, into whether or not the company provided reasonable security protection and whether or not it knowingly engaged in practices that kept the consumer in the dark.[58]

III. FACTS

Apple Pay is Apple's mobile payments service application that essentially allows a customer to replace his or her physical credit cards by using either the iPhone 6, iPhone 6 Plus, or iWatch to complete transactions.[59] Apple Pay's technology uses a near field communication ("NFC") to allow customers to pay at a checkout counter with fingerprint authentication.[60] In addition to the application, a consumer needs to add a debit or credit card to his or her iPhone, which will ultimately be stored in one's iTunes account.[61] Apple Pay

[56] *See id.* (considering the opinions of experts that litigation that requires Apple to appear in a courtroom could potentially provide precedent for how tech companies must behave).

[57] *See id.* (discussing the involvement of the Federal Trade Commission in investigation Apple's security measures). The question may become whether Apple was aware of the security flaw that led to the hack and ultimately did not fix it. *Id.*

[58] *See* Lapowsky, *supra* note 54 (predicting how the Federal Trade Commission may investigate whether Apple provided its customers reasonable security measures based on the sensitivity of the data and the significant risks of a data breach).

[59] *See* Dan Frommer, *The Complete Guide to Apple Pay*, QUARTZ (Oct.20, 2014), *archived at* http://perma.cc/D6G6-XEB5 (explaining how Apple Pay works and the specific Apple devices with which the app is compatible).

[60] *See* Matanda Doss, *Fingerprints, Apple Pay and Identity Theft*, VIRTUAL-STRATEGY MAGAZINE (Sept. 18, 2014), *archived at* http://perma.cc/B4NJ-VSKF (analyzing Apple Pay's NFC technology and the potential security risks to consumers). The NFC technology enables customers to pay at the point of sale machine with fingerprint authentication. *Id. See Your wallet. Without the wallet.*, APPLE, *archived at* http://perma.cc/HCJ7-E7VB (describing how Apple Pay works on the iPhone 6 and the security measures set forth so that the consumers credit or debit card information is protected). To pay, a customer simply holds the iPhone near the contactless reader with his or her finger on the Touch ID. *Id*.

[61] *See* Frommer, *supra* note 59 (listing exactly what a consumer needs to do in order to activate and begin using Apple Pay). In order to use Apple Pay, one needs to

works with several major credit-card companies including Visa, MasterCard, and American Express, as well as various U.S. banks, such as Citi, Chase, Bank of America, Capital One, and Wells Fargo.[62] In order to create a secure system, Apple Pay does not use one's actual credit card number and security digits (CVV), but instead generates a card number and security digits that only work one time.[63] The reasoning behind this is that if one's iPhone or Apple Watch were to be stolen, the customer would not need to cancel his or her credit cards.[64] Once the payment system is installed, customers are now able to approach the contactless reader at a participating vendor and simply hold up the iPhone to the device with their finger on the Touch ID fingerprint reader, a fingerprint-scanning feature.[65] Customers also have the option of inputting a PIN number, rather than using their fingerprint to authorize the transaction.[66] Since Apple Pay's release, Apple has tried to reassure the public and skeptics that

add a credit or debit card to the compatible device through the Passbook application. Apple pay stores the credit or debit accounts in one's iTunes account. *Id.*

[62] *See* Frommer, *supra* note 59 (stating which credit card services and banks Apple has established relationships with); *see also* Safwan Zaheer, *Why Banks Love Apple Pay*, PYMNTS (Oct. 20, 2014), *archived at* http://perma.cc/5FXN-Q8T9 (describing the relationship between Apple Pay and banks and how Apple's new payment system will help banks advance into the mobile payment generation and subsequently offer its consumers more options). Banks may have to share revenue with Apple, but splitting the profits is much better than losing the transaction and the customer entirely to a competitor. A bank's participation in Apple's digital commerce field will provide and create more opportunities for the bank to increase its transaction volume, introduce relevant products, and acquire new consumers. *Id*.

[63] *See* Anthony, *supra* note 7 (describing the security measures that Apple has set forth through Apple Pay's one-time "payment number" for consumer transactions); *see also* Weise, *supra* note 12 (expressing how Apple's "secure element" prevents thieves from accessing a customer's financial information). According to Rob Sadowski, Director of Technology Solutions for security company RSA, the security element is a "special area of secure encrypted storage controlled by the phone's operating system"). *See* Weise, *supra* note 12.

[64] *See* Anthony, *supra* note 7 (addressing the benefit of Apple Pay constantly using jumbled up numbers for every transaction rather than using the exact numbers on one's actual credit card).

[65] *See Your wallet. Without the wallet*, *supra* note 60 (explaining how to actually make a payment through Apple Pay by storing a credit or debit card on the iPhone 6 and holding the phone up to the contactless reader at a participating store in order to activate the Near Field Communication antenna in the phone).

[66] *See* Weise, *supra* note 12 (indicating that Apple gives consumers the option of using a PIN number or fingerprint to authorize transactions when using Apple Pay).

its mobile payment system is much safer and less vulnerable to security breaches than that of the traditional credit card.[67]

Although Apple Pay's security measures are convincing to some, others are not as satisfied with the digital fingerprint technology.[68] When Apple first introduced the Touch ID feature on the iPhone 5s, people had immediate concerns over privacy and identity tracking.[69] The company tried to put the skeptics at ease by announcing that the fingerprint scanner does not really store the actual images of users' fingerprints on the device, but rather only saves the "fingerprint data," which remains encrypted within the device's processor.[70] However, one day after the fingerprint-scanning feature was released, a hacker group called Chaos Computer Club claimed to have defeated Apple's Touch ID security by using a replicated fingerprint.[71] Apple

[67] *See* Weise, *supra* note 12 (discussing Tim Cook's statement that the magnetic stripe and exposed numbers on credit cards are outdated and more susceptible to fraud and theft). Apple Pay is effectively the same as the chip-and-PIN cards which contain a computer chip with encrypted financial information that generates a one-time authorization code and thus considered to be safer than the information encoded on the magnetic strip on the back of a credit card. *See* Weise, *supra* note 12.

[68] *See* Doss, *supra* note 60 (exploring concerns over the actual effectiveness and protection of Apple's digital fingerprint technology). Doss, the CEO of 5th Dimension Logistics, a global leader in the electronic payment industry, emphasized that once your fingerprint is stolen, you can never get it back, unlike a stolen credit card for which you can call the bank and get a replacement after securing your account. *Id.*

[69] *See* Chenda Ngak, *Should You Fear Apple's Fingerprint Scanner?*, CBS NEWS (Sept. 24, 2013), *archived at* http://perma.cc/VVZ2-URZR (stating the fears consumers had concerning privacy and hacking upon the introduction of Apple's Touch ID feature on the iPhone 5s).

[70] *See* Danny Yadron & Ian Sherr, *Apple: New iPhone Not Storing Fingerprints, Doesn't Like Sweat,* THE WALL STREET JOURNAL (Sept. 11, 2013), *archived at* http://perma.cc/7F87-MHTY (describing how the iPhone's Touch ID system does not save fingerprint data within the phone itself, thus keeping the device as secure as possible). The fingerprint data remains encrypted within the iPhone's processor until it is unlocked through the digital signature in order to make purchases in Apple's iTunes, iBooks or App stores. *Id.*

[71] *See* Joseph Steinberg, *Hackers Claim to Have Defeated Apple's Fingerprint Security*, FORBES (Sept. 23, 2013), *archived at* http://perma.cc/4EZS-857C (explaining how hackers asserted that they were able to defeat Apple's Touch ID system very quickly, which consequently raised concerns over major security vulnerabilities); *see also Chaos Computer Club*, CHAOS COMPUTER CLUB, *archived at* http://perma.cc/N3BZ-MVN7 (stating that Chaos Computer Club is Europe's largest group of hackers and security researches, which provides information about technical and societal issues, such as hactivism and data security). *But see* Kit

promised to fix any bugs in future software updates.[72] With the release of Apple Pay, which also significantly relies on a consumer's fingerprint as a security measure, it is evident that the mobile payment system may be alluring to hackers who have the potential to obtain, and perhaps control, a person's private financial information.[73]

Despite concerns over the strength of Apple's security system, millions of consumers are now in possession of the new iPhone 6 or 6 Plus and thus are consequently owners of a digital wallet.[74] The transition into the world of digital payments means that consumers will ultimately find themselves disregarding their physical wallets in exchange for a mobile payment system that allows one to pay with his or her phone at the checkout counter.[75] It is predicted that by 2018, mobile proximity payments in the United States, which in-

---

Eaton, *The Truth About The Newest iPhone Fingerprint Sensor Hack, And Why You Shouldn't Worry*, FAST COMPANY (Sept. 23, 2013), *archived at* http://perma.cc/YE6R-9LDW (highlighting that consumers should not be overly worried over Chaos Computer Club's claim that it hacked the iPhone 5S's Touch ID system because the method was not actually used through "easy everyday means" like the hacker group claimed). The complicated process of gaining access to the phone's fingerprint data involves the following:

> First, an image of a fingerprint is photographed from a glass surface at high resolution—2400 dpi. Then it is adjusted and improved using image editing software. Then a clean image of the print is printed using a laser printer, with a special setting for "thick" toner layers. This apparently creates an image on the printout that's made up of enough plastic toner that the ridges and folds in the fingerprint image are raised. Next, a positive fingerprint image is made from the printout, using a setting material like wood glue. Finally, someone breathes on the fake print, and taps it onto the iPhone 5S's sensor, which CCC claims recognizes it as a valid print.

Id.

[72] *See* Andy Greenberg, *German Hacker Group Says it's Broken the iPhone's TouchID Fingerprint Reader*, FORBES (Sept. 22, 2013), *archived at* http://perma.cc/Y62A-VR5S (recounting Apple's promise to fix bugs in its iOS7 operating system, involving the vulnerability of the lockscreen function and a locked phone's emergency call function).

[73] *See* Doss, *supra* note 60 (predicting that Apple Pay will be targeted by hackers, creating the possibility of a major security breach involving the fingerprint data).

[74] *See* Baig, *supra* note 8 (stating that with sales of more than 10 million new iPhones, consumers now have devices that double as digital wallets).

[75] *See* Baig, *supra* note 8 (citing how eBay's CEO, John Donahoe, believes the era of digital payments is upon us). Many individuals already use their phones to pay for coffee or a taxi ride, as well as buy music, movies, books, and apps, which are downloaded directly onto their devices. *See* Baig, *supra* note 8.

cludes payments made using a phone to make a physical transaction at the point of sale, will reach $118 billion, up from $3.5 billion in 2014.[76] Apple Pay may represent the first digital wallet or mobile payment system to succeed in the consumer market and the retail market.[77]

Apple's expansion into the mobile payment service market symbolizes a transition in the manner consumers make payments, but it also may mark a significant change in the way Apple is viewed as a company.[78] The question facing Apple extends beyond whether it is offering a consumer financial product or service through Apple Pay.[79] Depending on how Apple is defined under the Consumer Financial Protection Act, the company may be subject to regulation by the Consumer Financial Protection Bureau and subject to unfair, decep-

[76] *See* Baig, *supra* note 8 (explaining that eMarketer has said the number of mobile proximity payments in the U.S. will increase significantly between 2014 and 2018); *see also* Greg Petro, *With Apple Pay, Everyone Better Play*, FORBES (Nov. 2014), *archived at* http://perma.cc/EXT9-VQSR (highlighting the massive potential for consumer growth in the mobile payment market).

> In 2013, consumers spent only $1.6 billion through "contactless" mobile methods. Compare that to the $264.3 billion spent on e-commerce and the staggering $4.26 trillion consumers spent on traditional, in-store purchases. Right now, mobile payments account for a miniscule fraction of total payments for e-commerce and in-store purchases. The potential for growth on the consumer side of the market in the mobile payment sector is massive.

Id.

[77] *See* Petro, *supra* note 76 (discussing how Apple Pay is different from other major companies like Google, Verizon, and AT&T, who have all unsuccessfully tried to break into the mobile payment market); *see also* Baig, *supra* note 8 (indicating the difficulty of success in the digital wallet market and the fact that consumers have been making purchases with cash and plastic for decades).

[78] *See* Petro, *supra* note 76 (describing the public perception of Apple as a company).

[79] *See* Adam Levitin, *Apple Pay and the CFPB*, CREDIT SLIPS (Sept. 10, 2014), *archived at* http://perma.cc/63HP-ATQY (discussing Georgetown Law Professor Adam Levitin's analysis of how the introduction of Apple Pay may have consequently made Apple a "service provider" under the Consumer Financial Protection Act and therefore subject to examination by the Consumer Financial Protection Bureau); *see also* William Watts, *Law professor thinks Apple turned self into a regulated financial institution*, MARKETWATCH (Sept. 11, 2014), *archived at* http://perma.cc/H5R3-QC5D (analyzing Professor Adam Levitin's theory that Apple may have become a regulated entity through Apple Pay); *Money Services Business*, FINCEN, *archived at* http://perma.cc/N6C2-TPGQ (defining Money Services Business, which is a requirement of a business looking to transfer funds).

tive or abusive acts and practices (UDAAP).[80] Apple has yet to comment on this issue, but a spokesperson for the Consumer Financial Protection Bureau stated that "the agency will continue to closely monitor developments in mobile-payments technology in order to identify any consumer-protection issues."[81] Understanding the argument that Apple is or is not subject to financial regulation requires an analysis of the statute itself.[82]

IV. ANALYSIS

A. Apple's application to the Consumer Financial Protection Act

The possibility that the Consumer Financial Protection Act will regulate Apple revolves around if it meets the definition of a "service provider" under the Consumer Financial Protection Act.[83] The Consumer Financial Protection Bureau has authority over "covered persons" and "service providers."[84] Under the Act, a "covered person" refers to "any person that engages in offering or providing a consumer financial product or service."[85] Apple does not qualify under this definition because the financial product or service under scrutiny, Apple Pay, does not transmit funds in the same way as a com-

[80] *See* Levitin, *supra* note 79 (noting that if Apple is considered a "service provider" under the Consumer Financial Protection Act, it will consequently be subject to financial examination and regulation by the Consumer Financial Protection Bureau).
[81] *See* Watts, *supra* note 79 (quoting the Consumer Financial Protection Bureau's response to the notion that Apple may be subject to financial regulation due to its introduction of Apple Pay).
[82] *See* 12 U.S.C. § 5481 (defining terms under the Consumer Financial Protection Act).
[83] *See* 12 U.S.C. § 5481(26) (defining "service provider").
[84] *See* 12 U.S.C. § 5481(6), (26) (defining a "covered person" and "service provider" under the Consumer Financial Protection Act); *see also* Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 tit. 10 (2010) (stating the scope of coverage of the Consumer Financial Protection Bureau); Hletko & Hager, *supra* note 21 (discussing the Bureau's authority over covered persons and service providers, with a specific analysis into what is considered a service provider in this quickly technologically advancing age).
[85] *See* 12 U.S.C. § 5481(6) (defining the terms under the Consumer Financial Protection Act, including "covered person" and "service providers"); *see also* Hletko & Hager, *supra* note 21 (explaining that the Consumer Financial Protection Bureau has authority to regulate a covered person and a service provider as defined under the Act).

pany such as PayPal.[86] Additionally, at this current time, Apple does not have a MSB (money services business) license, which legally allows a business to transmit or convert money.[87] However, simply because Apple does not fulfill the requirements of a "covered person" does not automatically exempt it from being considered a "service provider."[88]

Although arguments can be made to dismiss the idea that Apple is a "service provider" under the Consumer Financial Protection Act, dissecting the language of the statute reveals that a stronger argument exists in favor of labeling Apple as a "service provider."[89] First, a "service provider" refers to one who "provides a material service to a covered person in connection with the offering or provision by such covered person of a consumer financial product or service."[90] Apple Pay provides a material service by giving card issuers another outlet where they can increase overall transaction volume in which additional benefits are given to existing and new customers.[91] Card issuers qualify as a "covered person" because they engage in the business of offering a consumer financial product—a credit card. [92] Therefore, Apple is making available a material service to banks or

[86] *See* 12 U.S.C. § 5481 (listing the definitions of terms used in the Consumer Financial Protection Act, along with the specifics of what is required to be considered a consumer financial product or service); *see also* Levitin, *supra* note 79 (discussing how Apple Pay is not in the same category as a company like PayPal because it does not offer money transfers).

[87] *See* 31 C.F.R. § 1010.100(ff) (2014) (defining Money Service Business); *see also* Levitin, *supra* note 79 (disclosing that Apple does not have a Money Service Business license at this time, suggesting that it is not a clear answer whether the company would be subject to regulation by the Consumer Protection Financial Bureau).

[88] *See* 12 U.S.C. § 5481 (defining a "covered person" as used within the Consumer Financial Protection Act).

[89] *See* 12 U.S.C. § 5481 (identifying Apple as a "service provider" as used within the Consumer Financial Protection Act).

[90] *See* 12 U.S.C. § 5481 (defining a "service provider" as used within the Consumer Financial Protection Act).

[91] *See* Zaheer, *supra* note 62 (describing the banks' benefits of entering into a partnership with Apple through Apple Pay and how those benefits will help maintain and improve the consumer base).

[92] *See* 12 U.S.C. § 5481 (defining a "covered person" under the Consumer Financial Protection Act); *see also* Levitin, *supra* note 79 (arguing that under the Consumer Financial Protection Act, Apple may be considered a service provider due to the fact that credit card issuers are labeled as covered persons). Additionally, by offering credit cards to consumers, banks are offering a "consumer financial product or service." *See* Levitin, *supra* note 79.

credit card companies by rendering them another outlet for their consumers to use their credit or debit cards in an easier fashion.[93] The definition of a "service provider" goes on to include a person that "participates in designing, operating, or maintaining the consumer financial product or service."[94] Apple has entered into partnerships with numerous credit card companies.[95] Because of Apple's extensive technological knowledge and the banks' limited understanding of the mobile payment world, it is clear that Apple helped to design, operate, and maintain the card payments that go through Apple Pay.[96] Apple had to consider what data was to be transmitted and how it was to be processed in order to maintain itself as a company consumers could trust.[97] Apple was not the middle man in providing Apple Pay's service to card issuers, but was rather fully involved in the process fulfilling that particular requirement of the "service provider" definition under the Consumer Financial Protection Act.[98]

The second part of the "service provider" definition includes one who "processes transactions relating to the consumer financial product or service."[99] Apple fits perfectly within this language since Apple Pay's purpose is to process transactions on a mobile device by

[93] *See* Zaheer, *supra* note 62 (revealing the significance of the partnership between card issuers and Apple and how this shift into the mobile payment arena could increase the overall transaction volume for banks).
[94] *See* 12 U.S.C. § 5481 (defining a "service provider" under the Consumer Financial Protection Act).
[95] *See Your wallet. Without the wallet, supra* note 60 (listing which credit card companies and banks work with Apple Pay on the iPhone 6, including Visa, MasterCard, and American Express).
[96] *See* 12 U.S.C. § 5481 (describing what is required to be labeled a "service provider" under the Consumer Financial Protection Act); *see also* Doss, *supra* note 60 (describing the NFC technology that Apple Pay utilizes in order to enable customer payments); *see also* Levitin, *supra* note 79 (suggesting that Apple participated in the design, operation, and maintaining of the Apple Pay data because the company has agreements with each card issuer or bank).
[97] *See* Heggestuen, *supra* note 9 (analyzing the importance of security to consumers, especially based on the more recent concerns of major data breaches at U.S. retailers); *see also* Levitin, *supra* note 79 (discussing Apple's role in managing what data was to be used and how it was to be transmitted through Apple Pay).
[98] *See* 12 U.S.C. § 5481 (defining a "service provider" as used within the Consumer Financial Protection Act).
[99] *See* 12 U.S.C. § 5481 (defining "service provider" under the Consumer Financial Protection Act).

taking the place of a physical credit or debit card.[100] However, the language specifically excludes those that are "unknowingly or incidentally transmitting or processing financial data in a manner that such data is undifferentiated from other types of data of the same form as the person transmits or processes."[101] The first part of this exclusion does not apply to Apple because the company is not "unknowingly or incidentally transmitting or processing financial data," but rather it is fully aware of how the data is formatted and used since it was involved in creating the service.[102] The second part of the exclusion that requires the data to be "undifferentiated from other types of data of the same form as the person transmits or processes" is also inapplicable because Apple created a special type of data that creates a distinctive device account number in place of storing the actual numbers of one's credit or debit card using NFC technology.[103] Since this device account number is encrypted, constantly changing, and stored in the iPhone's "Secure Element," it is in fact differentiated data.[104] However, even if this analysis of the carve-out is found to be off base, it does not completely discount the argument that Apple is a service provider since the carve-out applies only to the second description of a service provider under the Consumer Financial Protection Act.[105] Apple can still be labeled a service provider for simp-

[100] *See* Anthony, *supra* note 7 (revealing the purpose of Apple Pay and how it functions as a substitute for paying with a physical credit card).
[101] *See* 12 U.S.C. § 5481 (defining the carve-out of the "service provider" definition within the Consumer Financial Protection Act).
[102] *See* Levitin, *supra* note 79 (interpreting that Apple fully participated in the creation of the Apple Pay technology since banks and card issuers are naive as to the emerging mobile payment field); *see also* 12 U.S.C. § 5481 (specifying what is required to be a "service provider).
[103] *See* 12 U.S.C. § 5481 (specifying what is required to be a "service provider); *see* Weise, *supra* note 12 (describing the technology behind Apple Pay, including the NFC antenna built into the iPhone); *see also Your wallet. Without the wallet*, *supra* note 60 (elaborating on the security measures Apple created through a unique Device Account Number).
[104] *See Your wallet. Without the wallet*, *supra* note 60 (revealing the special chip in the iPhone, the Secure Element, where credit and debit card numbers are stored through encryption). According to Apple, one's credit and debit card numbers are never actually stored on the Apple servers. *Id.*
[105] *See* 12 U.S.C. § 5481(26) (stating that the carve-out in the "service provider" definition of the Consumer Financial Protection Act is only applicable to part ii of the definition); *see also* Levitin, *supra* note 79 (clarifying that even if Apple is not found to be a service provider based on part (ii) of the definition, the company can still qualify under part (i) since the carve-out does not apply).

ly participating in the designing, operating, and maintaining of Apple Pay.[106]

Although Apply Pay seems to fit within the definition of a "consumer financial product or service" under the Consumer Protection Act, some may argue that it is actually an electronic conduit service, which is not included in the definition of a financial product or service.[107] An electronic conduit service refers to the provision "of electronic data transmission, routing, intermediate or transient storage, or connections to a telecommunications system or network."[108] The argument that Apple is engaged in an electronic conduit service would have to be centered on the theory that Apple is neither in charge of formatting the data, nor is it in possession of the data.[109] Instead, Apple only helps to facilitate the existing transaction process for banks and card issuers on their own networks.[110] The fact that Apple is not directly advising the credit card's customers, charging interest, offering fraud protection, or providing other services characteristic of a bank supports the notion that perhaps Apple should not be regulated by the Consumer Protection Bureau because it is not on the same playing field as the other financially based companies.[111] Further, since the data has to be undifferentiated from other data of the same form in order to be included in the electronic conduit services definition, one would have to argue that the NFC technology used for Apple Pay on the iPhone 6 is also being used for other pur-

[106] *See* Levitin, *supra* note 79 (highlighting the argument that Apple is not just a common carrier transmitting data, but is rather involved in the process of determining what data to transmit and its format).
[107] *See* 12 U.S.C. § 5481(11), (5) (defining an "electronic conduit service" and a "financial product or service" as used in the Consumer Financial Protection Act).
[108] *See* 12 U.S.C. § 5481(11) (explaining what the term "electronic conduit services" means and what is not included within the definition).
[109] *See* 12 U.S.C. § 5481(11) (explaining what qualifies as an "electronic conduit service); *see also* Levitin, *supra* note 79 (indicating that in order for Apple to be free from regulation by the Consumer Financial Protection Bureau, Apple Pay would have to be considered an electronic conduit service rather than a service provider as defined under the Act). An electronic conduit service does not qualify as a "financial product or service" and thus would not be applicable to the service provider definition. *See* Levitin, *supra* note 79.
[110] *See* Frommer, *supra* note 59 (illustrating how Apple Pay functions on the iPhone 6 and how it offers customers another method to make transactions with their existing credit or debit cards).
[111] *See* Levitin, *supra* note 7979 (disclosing that Apple is not engaging in activities that suggest it is acting completely like a bank).

poses on the phone.[112] Currently, the payment data on the iPhone is the only type of data using NFC and Apple's "Secure Element" and therefore is differentiated from the operations of the iPhone's other features.[113] However, the iPhone's fingerprint ID technology, which is used for iTunes purchases and for unlocking the phone, serves the same purpose as the fingerprint technology utilized in Apple Pay.[114] This could spark the argument that the data being used for Apple Pay is in fact undifferentiated since the fingerprint verification is not solely being used for the payment service.[115] However, the encrypted data going through the iPhone's Secure Element is the force behind Apple Pay, while the fingerprint technology is merely an additional feature contributing to the overall purpose of the application.[116]

The Consumer Financial Protection Bureau's analysis of Apple Pay under the Act will be crucial for not only Apple's future, but also for its customers.[117] If the Bureau finds Apple to be a "service provider," the company will then be subject to regulation by the Bu-

[112] S*ee* 12 U.S.C. § 5481(11) (defining an electronic conduit service under the Consumer Financial Protection Act) *see also* Doss, *supra* note 60 (critiquing the NFC technology used in Apple Pay); *see also* Levitin, *supra* note 79 (explaining that Apple could use NFC technology for something else in the future besides Apple Pay and therefore Apple would not be using something unique, but rather undifferentiated data, which could perhaps consequently categorize the payment service as an electronic conduit service).

[113] *See* Levitin, *supra* note 79 (stating that Apple Pay is currently the only feature on the iPhone using the NFC technology); *see also Your wallet. Without the wallet*, *supra* note 60 (revealing that Apple Pay works by using a unique Device Account Number that is encrypted and stored in the "Secure Element," a specific security chip within the iPhone).

[114] *See* Doss, *supra* note 60 (explaining that Apple's fingerprint technology allows users to manage their phones with ease and speed by storing and encrypting the user's fingerprint data for his or her own phone); *see also* Yadron & Sherr, *supra* note 70 (stating that Apple's Touch ID system is not unique to Apple Pay, but is also incorporated into other features of the iPhone).

[115] *See* Levitin, *supra* note 79 (suggesting the argument that Apple Pay's data is not undifferentiated since it uses the same fingerprint technology that is used in other aspects of the iPhone). Consequently, Apple Pay could qualify as an electronic conduit service if the fingerprint technology is found to be undifferentiated data. *Id*.

[116] *See Your wallet. Without the wallet*, *supra* note 60 (explaining that Apple's Touch ID is a unique security feature of Apple Pay, but the "Secure Element" is the dedicated chip where one's credit and debit account numbers are stored).

[117] *See* Hletko & Hager, *supra* note 21 (citing to Congressional testimony from the Consumer Financial Protection Bureau regarding the possibility of reconsidering existing regulations due to technological advancements).

reau and UDAAP.[118] Additionally, Apple Pay will not be the only aspect of the company's regulation, but rather all of Apple's activities, whether financially based or not, will be subject to UDAAP.[119] This would be significantly new territory for Apple and the concern of potential examination by the Bureau could consequently alter the way Apple manages its company and its decisions to engage in a particular type of business.[120] While being federally regulated may hinder Apple's advanced creative process in the future, consumers may in fact benefit from the popular company being under the close watch of the Consumer Financial Protection Bureau.[121]

With the rise of data breaches in security systems at retail stores, as well as increased hacking in Apple's iPhones, the public is naturally concerned about the vulnerability of Apple Pay.[122] In his speech announcing Apple Pay and the iPhone 6, Tim Cook emphasized the "[s]ecure" system and technology involved in Apple Pay.[123] However, since some are not convinced of this alleged bulletproof security system, perhaps having Apple regulated by the Consumer Financial Protection Bureau will put consumers at ease knowing that

[118] *See* Hletko & Hager, *supra* note 21 (describing the Consumer Financial Protection Bureau's role and who it has the power to examine under the Consumer Financial Protection Act); *see also* Levitin, *supra* note 79 (detailing the implications for Apple if it is categorized as a "Service Provider" under the Act).

[119] *See* Levitin, *supra* note79 79 (stating that if the Bureau finds Apple to be a service provider, the entire corporation would then be vulnerable to UDAAP within any and every aspect of the company).

[120] *See* Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 tit. 10 (2010) (elaborating on the Consumer Financial Protection Bureau's powers and authority); *see also* Levitin, *supra* note 79 (interpreting the significance of the effects the Bureau's regulation and examination will have on Apple and its future endeavors); Watts, *supra* note 79 (discussing the power of the Consumer Financial Protection Bureau and how rules that apply to banks could also apply to Apple via Apple Pay).

[121] *See* Hletko & Hager, *supra* note 21 (discussing the consumer benefits of being protected by the Bureau).

[122] S*ee also* Doss, *supra* note 60 (exposing the potential security weaknesses of Apple Pay involving its NFC technology and fingerprint technology); *see also* Finkle & Hay, *supra* note 12 (describing cybersecurity researchers' discovery that a bug in Apple's iOS operating system made it vulnerable to hacking of sensitive data, including banking information and email login credentials); Godfrey, *supra* note 12 (highlighting the surge of cyber security attacks in 2013).

[123] *See* Doss, *supra* note 60 (recalling Tim Cook's speech where he revealed the security system backing Apple Pay).

the future-forward company is being carefully monitored.[124] Federal regulation will not only keep Apple attentive to the strength of its security system, but it will also result in a better opportunity for consumers to seek legal remedies if Apple violates UDAAP.[125]

It is reasonable to predict that security breaches will continue to occur in the future given the increase of reliability on technology to store personal and private data. Apple Pay appears to be an application that has the potential to be victim to a severe data breach, thus compromising the financial information of its numerous users.[126] Although the Consumer Financial Protection Act does provide remedies for UDAAP, regulating Apple's activity and examining its security measures may not be the first priority for the Bureau if Apple Pay ends up being categorized as a "service provider" and subject to examination.[127] However, the State Attorney General can still bring a civil action on behalf of Massachusetts Apple consumers if there is a massive Apple Pay data breach that the Consumer Financial Protection Bureau chooses not to address or pursue legally.[128] If a situation arose where several Apple consumers in Massachusetts had their Apple Pay data compromised due to a security breach, the Massachusetts Attorney General could bring an action that could potentially produce double or triple damages through M.G.L. 93A.[129] Thus,

[124] *See* Doss, *supra* note 60 (unveiling concerns for Apple consumers about the vulnerability of the fingerprint technology embedded in Apple Pay); *see also* Steinberg, *supra* note 71 (revealing that hackers were able to easily defeat Apple's Touch ID fingerprint technology in 2013 when it was first released).

[125] *See* 12 U.S.C. § 5551 (outlining the protections available for consumers under the Consumer Financial Protection Act).; *see also* Levitin, *supra* note 79 (hypothesizing the implications for Apple if it is considered a "service provider" under the Consumer Financial Protection Act, including the threat of being examined and regulated by the Consumer Financial Protection Bureau).

[126] *See* Doss, *supra* note 60 (detailing the consumer risk of a vulnerable Apple Pay system in which fingerprint data may easily be hacked, as it has been done in the past).

[127] *See* Levitin, *supra* note 79 (predicting that CFPB will probably not begin to examine Apple any time soon as there are more urgent matters and limited resources).

[128] *See* 12 U.S.C. § 5552 (stating that the attorney general of any State may bring a civil action in the name of that State to enforce the provisions of the Consumer Financial Protection Act).

[129] *See* MASS. GEN. LAWS 93A, § 9 (explaining that one can recover double or treble damages under 93A); *see also* Major Boston Restaurant Group That Failed to Secure Personal Data to Pay $110,000 Under Settlement with AG Coakley, *supra* note 39 (revealing that the Briar Group was forced to change its security measures as part of the settlement).

recognizing Apple Pay as a "service provider" under the Consumer Financial Protection Act will give consumers greater legal recourse, in the event of a data breach, under both federal and state law.

V. CONCLUSION

The future of Apple in the mobile payment evolution is yet to be determined in the eyes of the Consumer Financial Protection Bureau. However, Apple Pay appears to fit the "service provider" definition, which should submit it to examination and regulation by the Bureau. As the mobile payment arena develops and expands beyond Apple, the Bureau will be forced to acknowledge the existing security concerns surrounding the new payment system.