The Clearing House®

At the Center of Banking Since 1853®

Ensuring Consistent Consumer Protection for Data Security: Major Banks vs. Alternative Payment Providers

August 2015

Executive Summary

Over the last several years, the alternative payment provider (APP) industry has seen explosive growth, offering consumers new digital means to make payments and transfer money. This growth is only expected to continue, with some reports suggesting that mobile payments will grow annually by 60.8% through 2015, and that the peer-to-peer payments market will reach $17 billion in 2019. The APP market is also likely to grow through the increased use of so-called "Buy Buttons"—a means of integrating payment mechanisms into social media and search engine websites.

Although these new payment products generally require the collection and transfer of financial account and other sensitive personal information, the legal and regulatory frameworks designed to ensure the privacy and security of such information have not been revised to cover APP activities adequately. This regulatory failure has resulted in real consequences for customers, as reports have surfaced recently on data security and privacy lapses for APPs and mobile payment offerings.

Established banks have long offered payment solutions similar to those provided by APP companies. But banks, unlike APPs, are subject to extensive regulatory, supervisory, and enforcement scrutiny by their prudential regulators with respect to privacy and data security. APPs, by contrast, are providing their products and services by continuing to rely on the backbone of existing bank payment systems while capitalizing on innovations in communications platforms, thus generally managing to avoid the reach of the traditional financial regulators. For example, while both banks and most nonbank APPs are subject to the data security requirements established in the Gramm-Leach-Bliley Act (GLBA), the two groups are subject to quite different sets of implementing regulations and regulatory guidance, with banks subject to the more demanding standards issued by federal financial regulatory agencies and APPs subject to the more flexible regulations promulgated by the Federal Trade Commission (FTC). The result is not only lighter substantive requirements for APPs but also lower odds of facing enforcement actions and less prospect of substantial sanctions for violations. Other sources of APP data security requirements fail to compensate for this uneven regulatory landscape, both in terms of substantive requirements and the risks and consequences of enforcement actions.

Similarly, as a practical matter, APPs only face punishment for lax data security practices if they suffer an actual cybersecurity breach that is discovered by the government, because, unlike banks, APPs are not subject to regular examinations, enforcement actions, and other oversight by prudential regulators. While banks are subject to frequent examinations by their prudential regulators, which include data security-related examination, the FTC enforces its authority only through targeted, one-off civil investigative demands (CIDs). This lack of examination makes it is easier for APPs' security flaws to go undetected prior to a breach. And while both banks and APPs may be subject to injunctive relief for violations of the GLBA's requirements, only banks face a realistic possibility of civil money penalties, resulting in vastly different consequences for banks and nonbanks for violations of the same statute.

Even beyond the regulatory burden, banks often ultimately bear much of the customer service and fraud costs, even those associated with data security failures on the part of APPs.

Banks and APPs engaging in functionally similar activities should be subject to similar regulatory regimes. A regulatory level playing field of this sort is critical both to ensure that consumers enjoy consistent protection regardless of their choice of platform and to protect the safety and soundness of payment systems. To close the regulatory, enforcement, and examination gaps that exist today, we recommend:

» *Enhancing the substantive regulatory requirements.* The FTC should adopt enhanced GLBA Safeguards Rules, either limited to APPs or applicable more broadly to all the companies subject to the FTC's jurisdiction.

» *Using available examination authority.* The CFPB should issue rules defining larger participants of the APP industry, which would give the CFPB examination authority over those larger participants as defined. The CFPB or other regulators should also exercise any available examination authority they already have over APPs (such as those established as service providers to a financial institution).

» *Enforcing existing requirements.* For example, the FTC should enforce its GLBA Safeguards Rule more frequently for APPs, perhaps including through a CID sweep. For APPs that are federally registered as money services businesses with the Financial Crimes and Enforcement Network (FinCEN), FinCEN should enforce existing guidance that would require those APPs to report actual or attempted data breaches to the government in the form of suspicious activity reports (SARs).

Enacting legislation establishing additional data security requirements for APPs.

» The Data Security Act of 2015 (S. 961 and H.R. 2205) would establish flexible and common-sense standards, based on the GLBA Interagency Guidelines, for firms of all sizes to follow in order to secure consumers' sensitive financial information and prevent breaches. These bills would also give the FTC express enforcement authority in this area, while making clear that the standards are not applicable to financial institutions already subject to data security regulation by the prudential regulators.

» In order to exercise any new authority successfully, the FTC would also need more resources to properly staff investigations and enforcement actions.

» Additional legislation might make clear that APPs are subject to the same type of scrutiny with respect to data security as banks, such as by directly giving the FTC or CFPB examination authority (without requiring further regulations to do so), or by directly requiring the CFPB to enact rules defining larger participants in the APP industry.

Table of Contents

I. Introduction

Over the last several years, the alternative payment provider (APP) industry has seen explosive growth, offering consumers new digital means to pay merchants, exchange money with friends, and use their wallets in other contexts. Although these new payment products generally require the collection and transfer of financial account and other sensitive personal information, the legal and regulatory frameworks designed to ensure the privacy and security of such information have not been revised to cover APP activities adequately. Established banks have long offered payment solutions such as Automated Clearing House (ACH) transfers, checks, and online bill-pay systems, and they have increasingly offered digital payment systems like those provided by APP companies. But banks, unlike APP providers, are subject to extensive regulatory, supervisory, and enforcement scrutiny with respect to privacy and data security. Thus, while APPs and banks increasingly compete head to head, APPs face dramatically less regulatory oversight of their data security and privacy practices than do banks, with real consequences for their customers. [1]

While this gap has existed for years, it has become more problematic in recent years as the APP industry has grown, leading to increased risk of security lapses and increased consequences of such lapses. Improper data security protections could lead not only to unauthorized disclosure of sensitive personal or financial information stored by an APP, but could also lead to fraudulent transactions conducted through the APP. Both risks are important to consumers.[2] And ultimately, banks often bear the costs of closing/replacing cards or accounts, investigating incidents of fraud, refunding fraudulent charges, and monitoring accounts for fraudulent activities.

Part I of this white paper briefly describes the growth of the APP industry, noting some examples of recently reported data security lapses. It then compares large banks and APPs when it comes to regulatory, supervisory, and enforcement scrutiny concerning data security. Part II addresses the substantial gaps in substantive data security requirements the two groups bear. Part III describes gaps in supervision and enforcement. These comparisons show that APPs operate under markedly lighter legal and regulatory regimes for data security in every dimension. Part IV explains the financial consequences this has for banks, already playing on an uneven regulatory

1 This concern was acknowledged by Comptroller of the Currency Thomas Curry during remarks before the BITS Emerging Payments Forum on June 3, 2015. He noted that "regulation adds significant value in the areas that we're discussing today [i.e., payment technologies and cybersecurity]. For example, efforts are well underway to bring e-commerce and emerging payments systems deployed by non-bank players under greater regulatory scrutiny . . . [to] ensure a more level playing field and protections for customers of non-banks. Certainly, they deserve no less." Thomas J. Curry, Comptroller of the Currency, Remarks Before the BITS Emerging Payments Form (June 3, 2015), available at **http://www.occ.gov/news-issuances/speeches/2015/pub-speech-2015-78.pdf**.

2 *See, e.g.*, Federal Reserve Board, *Consumers and Mobile Financial Services* at 14 (Mar. 2015), **http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201503.pdf** (noting that, of those users who did not use mobile banking due to concerns about security, 17% reported concerns about their phone being hacked, 22% were concerned about someone intercepting their data, while less than 10% each were concerned about losing their phone or their phone being stolen, someone using their phone without permission to access their account, company misuse of personal information, and malware/viruses being installed on the user's phone, while 43% were concerned about all of the stated reasons).

playing field, as banks end up having to pay the price for APPs' data security failures. Finally, Part V offers a set of recommendations designed to help ensure that when consumers use APPs they are no less protected with respect to data security as they are when they use products and services offered by banks.

II. The Alternative Payment Provider Industry: Explosive Growth but Data Security Lapses

The APP industry includes many nonbank companies offering alternative payment solutions. These solutions range from ones offered by large tech companies, such as Apple Pay, Google Wallet, and Facebook Messenger;[3] to successful payment-focused startups offering payment systems as the core of their business, such as point-of-sale solutions providers Square, LevelUp, and Kash,[4] peer-to-peer (P2P) money transfer services PayPal and Venmo,[5] entities that act as a front-end to the ACH rail such as Knox Payments,[6] and application program interfaces Stripe and Plaid;[7] to a number of earlier-stage startups seeking to introduce payment innovations and asking consumers to entrust their money to them.

The alternative payments market has seen substantial growth in the last few years,

3 Apple Pay is a mobile payment service that lets Apple mobile devices make payments by aggregating, digitizing, and replacing magnetic stripe cards. Apple, Apple Pay, **http://www.apple.com/apple-pay/**. Google Wallet provides a similar feature, providing a mobile application that operates as a "virtual wallet" by linking to underlying payment credentials (including credit, debit, prepaid, or gift cards) that can be used to redeem sales promotions or access loyalty program information, and allows consumers to make payments online or using mobile devices at retail locations. The Clearing House, Developing a Comprehensive Regulatory Framework for Electronic Payments at 18 (Apr. 2013). Facebook's offering allows users to send payments to other Facebook users through the Facebook Messenger application, similar to PayPal, Venmo, and Square Cash, discussed below. Press Release, Facebook, Send Money to Friends in Messenger (Mar. 17, 2015), **http://newsroom.fb.com/news/2015/03/send-money-to-friends-in-messenger/**.

4 Square, LevelUp, and Kash focus on offering point-of-sale solutions. Square provides mobile point-of-sale tools to allow users to turn their iPads or iPhones into mobile credit card readers. See Square, Square Register, **https://squareup.com/register**; Square, Square Stand, **https://squareup.com/stand**; Square, Square Reader, **https://squareup.com/reader**. LevelUp provides a mobile app that consumers may download to mobile devices and link to credit or debit cards. Once linked to a consumer's payment card, LevelUp can be used to display a "QR" or quick response code on the mobile device to make payments at participating merchants. The Clearing House, Developing a Comprehensive Regulatory Framework for Electronic Payments at 16. Kash offers a similar mobile point-of-sale payment option, by allowing users with the Kash mobile application to connect their bank account using their online banking log-in information. Kash, How it Works, **https://withkash.com/merchant/howitworks**; Ruth Reader, Kash brings $2M to the mobile payments arena and launches amid Apple Pay's rollout, Venture Beat (Nov. 4, 2014), **http://venturebeat.com/2014/11/04/kash-brings-2m-to-the-mobile-payments-arena-and-launches-amid-apple-pays-rollout/**.

5 PayPal is an e-commerce business that allows consumers and businesses to make and receive payments through online P2P transfers, retail point-of-sale purchase processing, online and mobile payment processing, and certain affiliated e-commerce sites, using linked bank accounts or credit/debit cards. The Clearing House, Developing a Comprehensive Regulatory Framework for Electronic Payments at 26. Venmo (recently acquired by PayPal through PayPal's acquisition of Venmo parent Braintree) offers a similar P2P money transfer service, through linked bank accounts or payment cards, based in a social media application. Venmo, How it Works, **https://venmo.com/about/product/**. Square also offers a similar service, Square Cash (which powers, among other things, Snapcash, a money transfer service through the Snapchat application). Julia Boorstin, Can Square Cash replace $1 trillion in checks?, CNBC (Mar. 23, 2015), **http://www.cnbc.com/id/102527065**; Snapchat Blog, Introducing Snapcash (Nov. 17, 2014), **http://blog.snapchat.com/post/102895720555/introducing-snapcash**.

6 Knox Payments is intended to offer an alternative front end to the ACH money transfer process. See Harrison Weber, Knox Payments launches with $900K to speed up painfully slow online check-outs, Venture Beat (Feb. 26, 2014), **http://venturebeat.com/2014/02/26/knox-payments-launches-with-900k-to-speed-up-painfully-slow-online-check-outs/**; Knox Payments, Home Page, **https://knoxpayments.com/**.

7 Stripe and Plaid offer APIs, or application program interfaces, for developers to incorporate into their applications for the acceptance of payments. Stripe, About, **https://stripe.com/about**; Plaid, Home Page, **https://www.plaid.com/**.

reflecting increasing amounts of consumer funds and consumer data entrusted to APPs. For example:

» **Growth of PayPal.** In Q1 2010, PayPal processed a net total payment volume of just over $20 billion, which more than tripled by Q4 2014.[8] In that same period, mobile payments on PayPal grew from $750 *million* annually in 2010 to $46 billion in 2014.[9]

» **Growth of P2P market.** In 2010, only 4% of web-connected adults used P2P mobile payments,[10] and some estimates suggested that U.S. households spent an average of just $8 per year on P2P transactions using mobile channels at that time.[11] In July 2013, just over a year after its public launch, Venmo's user figures were reportedly growing at a rate of 15% every month.[12] The mobile P2P payment market totaled a reported $5.2 billion in 2014.[13] As of March 2015, the P2P market is expected to reach $17 billion in 2019.[14]

» **Growth of APPs for online transactions.** In January 2014, it was estimated that APPs will account for 59% of online transactions in 2017, up from 43% in 2012.[15]

» **Growth of e-wallets.** According to that same January 2014 report, e-wallets are estimated to equal cards in terms of market share by 2017, with each predicted to have a 41% share of the payments market with $1,656 billion in payments in 2017 (as compared to $295 billion in 2012).[16]

» **Growth of mobile payments generally.** In 2010, $16 billion in transactions were processed as mobile payments.[17] This increased to $46 billion in 2011 and $81 billion in 2012. In December 2014, 22% of mobile phone owners reported having made a mobile payment in the prior year, compared with 17% in 2013, 15% in 2012, and only 12% in 2011.[18] When limited to smart phone users only, these numbers grow, with 28% of smartphone users having made mobile payments in 2014, up from 23-24% in each of the prior three years.[19] Some reports suggest that mobile pay-

8 Statista, PayPal's total payment volume from 1st quarter 2010 to 1st quarter 2015 (in billion U.S. dollars), http://www.statista.com/statistics/277841/paypals-total-payment-volume/.

9 Statista, PayPal's annual mobile payment volume from 2008 to 2014 9in million U.S. dollars), http://www.statista.com/statistics/277819/paypals-annual-mobile-payment-volume/.

10 Becky Yerak, Smart-phone money transfers are a growing business; trends, Providence Journal (Dec. 18, 2011).

11 Marc Rapport, Advancing from In-Person Cash to Electronic, Credit Union Times (Jan. 12, 2011).

12 Natalie Robehmed, Venmo: The Future of Payments For You and Your Company, Forbes (July 2, 2013), http://www.forbes.com/sites/natalierobehmed/2013/07/02/venmo-the-future-of-payments-for-you-and-your-company/.

13 Trevor Nath, How Safe is Venmo and Why is it Free?, Investopedia (Mar. 24, 2015), http://www.investopedia.com/articles/personal-finance/032415/how-safe-venmo-and-why-it-free.asp.

14 Id.

15 Alternative payments to overtake credit and debit cards globally, Payments Card & Mobile (Jan. 22, 2014), http://www.paymentscardsandmobile.com/alternative-payments-overtake-credit-debit-card-payments-globally/.

16 Id.

17 Crowe Horwath, The History and Use of Alternative Payment Systems and the Risks They Present at 21 (Dec. 11, 2013), http://www.crowehorwath.com/folio-pdf/TheHistoryUseAlternativePaymentSystemsWebinar_RISK14119D.pdf.

18 Federal Reserve Board, Consumers and Mobile Financial Services at 1, 5 (Mar. 2015), http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201503.pdf. For the purpose of these statistics, mobile payments includes payments made by accessing a web page through a web browser on a mobile device, sending a text message, or using a downloadable application. Id. at 14.

19 Id. at 2, 5.

ments are expected to grow annually by 60.8% through 2015. [20]

» **Exploration of "Buy" Buttons.** A number of social media sites and search engines have recently begun exploring the use of "Buy Buttons," which are intended to allow users to buy products without leaving the application or site and, according to Twitter's head of commerce, serve as a "bridge between a consumer wanting something and getting it."[21] Twitter started testing its Buy Button last September through a partnership with APP Stripe, which allows users to buy, among other things, tickets for sporting events and concerts directly through Twitter.[22] Facebook has launched a similar partnership with Stripe,[23] while Google and Pinterest have acknowledged they have plans to integrate buying capability into search ads and "pinned" images, respectively.[24]

Along with this rapid growth have come a series of data security and privacy lapses. Shortly after Google Wallet was launched, for example, a security firm discovered a way to force Google Wallet to reset itself and prompt the user for a new PIN, allowing anyone who gains access to a phone (without lock screen protection) to change the Google Wallet PIN and make all funds on the wallet available.[25] And, as recently as the end of 2014, there were reports of various security vulnerabilities in PayPal, a veteran payment provider compared with many of the other APPs. These vulnerabilities included the ability to override two-factor authentication, and a means to bypass the service's "Cross-Site Request Forgery Protection Authorization System." [26]

Venmo, which processed $700 million in payments in Q3 2014 alone, has also been the subject of criticism, following a recent article which documented user complaints about fraud in the service tied to security failures.[27] The article highlighted the fact that key account information can be changed without sending a notice email to the original email address associated with the account, a key security feature routinely implemented by banks, thus allowing a hacker to gain access to an account and transfer money to another account completely undetected by the user.[28] This is

20 Capgemini and Royal Bank of Scotland, World Payments Report 2014 at 12.

21 Sarah Frier, Twitter Testing Buy Button as E-Commerce Plans Take Shape, Bloomberg (Sept. 8, 2014), http://www.bloomberg.com/news/articles/2014-09-08/twitter-testing-buy-button-as-e-commerce-plans-take-shape.

22 Sarah Frier, Twitter Buy Button Pops Up for Event Tickets, Bloomberg (Apr. 20, 2015), http://www.bloomberg.com/news/articles/2015-04-20/twitter-buy-button-pops-up-for-event-tickets.

23 Kurt Wagner and Jason Del Ray, Facebook Is Partnering With Stripe to Power "Buy" Button, Re/code (Sept. 25, 2014), http://recode.net/2014/09/25/facebook-is-partnering-with-stripe-to-power-buy-button/. See also Conor Dougherty and Hiroko Tabuchi, New, Simple 'Buy' Buttons Aim to Entice Mobile Shoppers, New York Times (July 5, 2015), http://www.nytimes.com/2015/07/06/technology/new-simple-buy-buttons-aim-to-entice-mobile-shoppers.html?mwrsm=Email&_r=0.

24 Jason Del Rey, Why 'Buy' Buttons Will Pose Big Challenges for Google, Facebook, Pinterest, and Twitter, Re/code, (June 14, 2015), http://recode.net/2015/06/14/why-buy-buttons-will-pose-big-challenges-for-google-facebook-pinterest-and-twitter/.

25 Andrew Tarantola, Google Wallet Hacked Again, Gizmodo (Feb. 9, 2012), http://gizmodo.com/5883913/google-wallet-has-been-hacked-again-now-you-should-panic.

26 Thomas Halleck, PayPal Accounts Hacked With a Click: Engineer Uncovers Potential Security Breach, International Business Times (Dec. 4, 2014), http://www.ibtimes.com/paypal-accounts-hacked-click-engineer-uncovers-potential-security-breach-1735158.

27 Allison Griswold, Venmo Money, Venmo Problems, Slate (May 14, 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.

28 Id. The article indicates that it was the user's bank, not Venmo, that alerted the user to the pending transfer.

a fairly basic security mistake that financial regulators would not stand for when it comes to regulated banks. In fact, in the Federal Financial Institutions Examination Council (FFIEC) 2011 guidance *Supplement to Authentication in an Internet Banking Environment*, the FFIEC makes clear that one of its "specific supervisory expectations" is that banks implement layered security at different points in transactions to ensure that multiple controls compensate for a weakness in one control, including through the use of "enhanced control over changes to account maintenance activities performed by customers."[29] This would presumably include changes to an account's associated email address.

In another example of an APP security lapse, Starbucks recently acknowledged that criminals have been siphoning money away from victims' credit cards and bank and PayPal accounts through their Starbucks cards.[30] Starbucks processed $2 billion in mobile payment transactions last year through the Starbucks application. It has thus far denied that the recent compromises were the result of a cybersecurity breach,[31] and reporting suggests this was actually the result of users' accounts (with their linked bank accounts) being hacked because the users used the same username and password combinations as used for other, breached accounts.[32] Even then, this exhibits the danger of linked bank accounts where the accounts lack even the most basic of additional security measures (such as those mandated by the FFIEC Authentication Guidance) to prevent unauthorized use.[33] And, in an apparently unrelated issue, a security researcher exploited a bug in the Starbucks gift card and yet faced extensive difficulty and delay in receiving a response to his reporting of the bug to Starbucks and in the company's ultimately fixing it. [34]

Both the failure to implement even the most basic of layered security measures when dealing with linked bank accounts and financial transactions, and the lack of receptiveness to receiving and properly responding to reports of identified bugs, is exemplary of the naiveté of some of these APPs with respect to security considerations, and the lack of motivation to take security seriously. These lapses are particularly striking in examples like Starbucks, which is "viewed by payments analysts and industry trade reports as an *example of successful implementation* of a closed-loop mobile payment model."[35]

In addition to fraudulent transactions, APPs collect a significant amount of customer data,

29 FFIEC, Supplement to Authentication in an Internet Banking Environment (2011), available at **https://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20%28FFIEC%20Formated%29.pdf** .

30 Jose Pagliery, Hackers are draining bank accounts via the Starbucks app, CNN (May 13, 2015), **http://money.cnn.com/2015/05/13/technology/hackers-starbucks-app/index.html**; Bob Sullivan, EXCLUSIVE: Hackers target Starbucks mobile users, steal from linked credit cards without knowing account number, bobsullivan.net (May 11, 2015), **https://bobsullivan.net/cybercrime/identity-theft/exclusive-hackers-target-starbucks-mobile-users-steal-from-linked-credit-cards-without-knowing-account-number/**.

31 Sullivan, supra.

32 Starbucks Hacked? No, But You Might Be, Krebs on Security (May 18, 2015) **http://krebsonsecurity.com/2015/05/starbucks-hacked-no-but-you-might-be/**.

33 FFIEC, Supplement to Authentication in an Internet Banking Environment.

34 Dan Goodin, Researcher who exploits bug in Starbucks gift cards gets rebuke, not love, Ars Technica (May 24, 2015), **http://arstechnica.com/security/2015/05/researcher-who-exploits-bug-in-starbucks-gift-cards-gets-rebuke-not-love/**.

35 Susan Pandy, Technology and Security Considerations for Mobile Contactless Payments at the Point-of-Sale in the U.S., Summary of June 18-19, 2013 Mobile Payments Industry Workgroup Meeting at 8, Federal Reserve Bank of Boston (Nov. 8, 2013), available at **http://www.bostonfed.org/bankinfo/payment-strategies/publications/2013/summary-of-mpiw-meeting-june-2013.pdf** (emphasis added).

which is at risk of being stolen by hackers if insufficient security precautions are used to protect the data. For example, during the early pilot stages of APP CurrentC,[36] the company announced that it had been hacked, resulting in the theft of the email addresses of anyone who had signed up for the program.[37]

36 CurrentC is an attempted Apple Pay rival launched by retailer consortium Merchant Customer Exchange. Jose Pagliery, Apple Pay rival CurrentC just got hacked, CNN (Oct. 29, 2014), http://money.cnn.com/2014/10/29/technology/security/currentc-app-hacked/.

37 Id.

III. APPs Are Subject to Dramatically Lighter Regulatory Requirements than Are Major Banks

APP companies hold many of the same types of data and perform many of the same types of consumer payment transactions as major banks. Yet the substantive regulations that govern banks' data security practices are markedly more stringent than those applicable to APPs. This is in line with the overall regulatory context for financial institutions as compared with other consumer products. Banks have long been subject to extensive regulatory, supervisory, and enforcement scrutiny by their prudential regulators, a framework which has naturally evolved to include scrutiny with respect to privacy and data security.

APPs, by contrast, are providing their products and services by continuing to rely on the backbone of existing bank payment systems while capitalizing on innovations in communications platforms, thus generally managing to avoid the reach of the traditional financial regulators.[38] Instead, to the extent APPs are regulated, they are subject predominantly to the jurisdiction of the Federal Trade Commission (FTC), an agency with less authority and resources than financial regulators.

THE GRAMM-LEACH-BLILEY ACT

While both banks and most, if not all, nonbank APPs are subject to the data security requirements established in the Gramm-Leach-Bliley Act (GLBA), the two groups are subject to quite different sets of implementing regulations and regulatory guidance. Banks are subject to the more demanding *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*, adopted jointly by the federal financial regulatory agencies, while APPs are subject to the more flexible Safeguards Rule promulgated by the FTC. The result is not only lighter substantive requirements for APPs but also lower odds of facing enforcement actions and less prospect of substantial sanctions for violations.

Prudential Regulators and the Interagency Guidelines

Bank GLBA data security requirements have been laid out in the prudential regulators' *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*

38 This is despite keen interest by many of the financial regulators in mobile payments and APPs. In the Mobile Payments Industry Workgroup 2014 update on the mobile payments regulatory landscape, Susan Pandy, the Director of Payment Strategies for the Federal Reserve Bank of Boston, described the "role of regulators in mobile payments," which essentially outlined the various ways in which federal regulators are monitoring trends, conducting studies, and engaging in dialogue around the area of mobile payments. Susan Pandy, Update on the U.S. Regulatory Landscape for Mobile Payments, Summary of Meeting between Mobile Payments Industry Workgroup (MPIW) and Federal and State Regulators at 4-8, Federal Reserve Bank of Atlanta and Federal Reserve Bank of Boston (Aug. 18, 2014), available at http://www.bostonfed.org/bankinfo/payment-strategies/publications/2014/summary-of-mpiw-meeting-may-2014.pdf. In doing so, Pandy essentially acknowledged that federal regulators lack the authority to act in this area, despite a keen interest in doing so. Only in the discussion of the CFPB's role, which we discuss further below, did the summary note that the regulator is evaluating whether there is a need for mobile-specific rules.

(Interagency Guidelines).[39] The Interagency Guidelines require each bank to implement a comprehensive written information security program, appropriate to its size and complexity and the nature and scope of its activities.[40] The program must be designed to ensure the security and confidentiality of customer information; protect such information against any anticipated threats, and unauthorized access to or use of such information; and ensure the proper disposal of customer information.[41]

Financial institutions' information security programs must include six components: (1) board of directors' involvement, including at least annual reporting to the board; (2) risk assessment; (3) risk management and control; (4) oversight of service providers; (5) an incident response program; and (6) periodic updating.

Board of directors. The board of directors "or an appropriate committee of the board" must (i) "approve the bank's information security program"; (ii) "oversee the development, implementation, and maintenance of the bank's information security program, including assigning specific responsibility for its implementation"; and (iii) review at least annual reports from management on the "overall status of the information security program and the bank's compliance" with the Interagency Guidelines, including "issues such as risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes."[42]

Risk assessment. Financial institutions are required (i) "to identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems"; (ii) "to assess the likelihood and potential damage of these threats, taking into account the sensitivity of customer information"; and (iii) "to assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks."[43]

Risk management and control. Financial institutions must (i) consider whether, given the risks they face and the complexity of their operations, a number of security controls would be appropriate: (a) access controls ; (b) physical access restrictions; (c) encryption, in transit or at rest; (d) procedures to ensure that modifications to customer information systems are consistent with the information security program; (e) dual control procedures, such as segregation of duties and background checks; (f) monitoring to detect intrusions and attempted intrusions; (g) protocols for responding in the event of intrusions, including reports to regulatory and law enforcement agencies; (h) protection against environmental hazards, such as fire or water damage; (ii) train staff to implement the information security program; (iii) regularly test key controls, systems and procedures in their information security program, using independent staff from inside or outside the institution; and (iv) maintain appropriate

39 12 C.F.R. Part 30, App. B (as incorporated into the OCC regulations for national banks). In additional to national banks, the Interagency Guidelines apply to member banks of the Federal Reserve System, banks and savings associations insured by the Federal Deposit Insurance Corporation, federally-insured credit unions, and broker-dealers, investment companies, and investment advisers.

40 Id. § II.A.

41 Id. § II.B.

42 Id. § III.A, F.

43 Id. § III.B.

procedures to properly dispose of customer information. [44]

Oversight of service providers. Financial institutions are required (i) to exercise "appropriate due diligence" in selecting service providers; (ii) to require by contract that service providers "implement appropriate measures designed to meet the objectives" of the GLBA guidelines; and (iii) "[w]here indicated by the bank's risk assessment, monitor its service providers to confirm that they have satisfied th[ose contractual] obligations," including by reviewing audits, summaries of test results, or other equivalent evaluations.[45]

Response program. In the event of "unauthorized access to sensitive customer information," financial institutions must "conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused." "Sensitive customer information," for these purposes, means "a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account." If such misuse has occurred or "is reasonably possible," the financial institution should notify affected customers by means "designed to ensure that a customer can reasonably be expected to receive" the notice. The notice should include a description of the intrusion, a telephone number to call for assistance, recommendations about fraud alerts, identity theft resources, and checking with credit reporting agencies. [46]

Updating. Financial institutions should evaluate and adjust their information security programs "in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the bank's own business arrangements," including outsourcing arrangements and customer information systems. [47]

When it comes to regulators' expectations, the Interagency Guidelines are supplemented by various guidance documents issued by the FFIEC member agencies. These include FFIEC's Information Technology Examination Handbook, especially its Information Security, Outsourcing Technology Services, and Supervising Technology Service Providers booklets [48] as well as topical bulletins that include information security components, [49] and other guidance documents, such as the recently released Cybersecurity Assessment Tool. [50] The IT Examination Handbook's Information Security booklet alone contains nearly 90 pages

44 Id. § III.C.

45 Id. § III.D.

46 Id. App. B, Supp. A. The response program component of the Interagency Guidelines was elaborated separately in Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. See 70 Fed. Register 15736 (Mar. 29, 2005).

47 Id. App. B § III.E.

48 These booklets, along with the other IT Examination Handbook booklets, are available at **http://ithandbook.ffiec.gov/it-booklets.aspx**.

49 See, e.g., Risk Management Guidance, OCC Bulletin 2013-29 (Oct. 30, 2013), available at **http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html** (providing guidance for assessing and managing risks associated with third-party relationships, including information security, management of information systems, and incident-reporting and management programs); FFIEC, Supplement to Authentication in an Internet Banking Environment.

50 FFIEC, Cybersecurity Assessment Tool, **https://www.ffiec.gov/cyberassessmenttool.htm**.

of detailed information security guidance, including information on implementation of specific security controls (ranging from remote access to encryption key management) and security monitoring. [51]

The Federal Trade Commission's Safeguards Rule

While APPs are likely subject to the GLBA's data security requirements, [52] as nonbank institutions APPs do not have to follow the Interagency Guidelines. Instead, they are subject to the more general requirements of the FTC's GLBA Safeguards Rule. [53] The Safeguards Rule's requirements are not only less robust than the Interagency Guidelines' requirements; they also come without the additional detailed expectations set out in the FFIEC's IT Examination Handbook and in other FFIEC agency guidance documents.

The Safeguards Rule requires covered APPs to implement a written information security program containing administrative, technical, and physical safeguards appropriate to the company's size, complexity, activities, and maintenance of sensitive customer information. [54] Similar to the program required by the Interagency Guidelines, the program mandated by the Safeguards Rule is to be designed to ensure the security and confidentiality of customer information, and to protect against threats or unauthorized access that could result in substantial customer harm or inconvenience. [55]

The Safeguards Rule outlines five basic required elements for developing, implementing, and maintaining an information security program: (1) designate an employee to coordinate the program; (2) identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of such safeguards; (3) design and implement information safeguards to control risks identified through regular assessments, and regularly test or monitor the effectiveness of key controls; (4) oversee service providers, including taking reasonable steps to retain providers that are capable of maintaining appropriate safeguards and contractual provisions requiring such safeguards; and (5) evaluate and adjust the program in light of testing and monitoring, material changes to the business, or other circumstances with a material impact on the information security program. [56]

Some Key Distinctions

The differences between the data security requirements imposed on banks by the

51 FFIEC, Information Security (July 2006), available at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf.

52 15 U.S.C. § 6809(3)(A) (defining "financial institution" subject to the GLBA as "any institution the business of which is engaging in financial activities as described in section 1843 (k) of title 12," which includes, for example, "transferring . . . money"). Whether each specific APP falls under this definition requires a fact-specific inquiry into the functionality of the APP. To the extent any APP is not subject to the GLBA's data security requirements, this would of course only serve to widen the gap between major banks and APPs in terms of data security requirements.

53 Standards for Safeguarding Customer Information, 16 C.F.R. Part 314.

54 Id. § 314.3(a).

55 Id. § 314.3(b). Proper disposal of records is covered separately under the FTC's Disposal Rule under the Fair and Accurate Credit Transactions Act. Id. Part 682.

56 Id. § 314.4.

Interagency Guidelines and those applicable to APPs under the FTC's Safeguards Rule are numerous. Here we highlight six fundamental ones.

First, the difference in the level of detail between the two regimes has real implications for types of data security precautions regulators can reasonably demand from banks, on the one hand, as compared to APPs, on the other. For example, an APP subject to an investigation and/or potential enforcement action by the FTC could quite reasonably argue that there are no specific requirements for technical controls they are required to employ to control identified risks. [57] By contrast, no reasonable bank could argue that it should not at least consider access controls, encryption, segregation of duties, and other controls that are explicitly identified in the Interagency Guidelines.[58] This gap is only compounded by the detailed supplemental guidance from the FFIEC in the form of individual guidance documents and the IT Examination Handbook.

Second, the Interagency Guidelines require involvement from bank leadership at the highest level, including boards of directors and senior business management. [59] As noted above, a bank's board of directors must participate by approving and overseeing the development, implementation, and maintenance of the information security program, including through the receipt of annual reports on the program's status.[60] By contrast, under the Safeguards Rule, APPs can simply designate an employee to coordinate the information security program and train their employees, without having to involve their senior leadership.

Third, recognizing the significant risk posed by insider threats, the Interagency Guidelines require that banks at least consider using employee background checks for employees with responsibilities for or access to customer information. The FFIEC Information Security Booklet further states that financial institutions "should have a process to verify job application information on all new employees," and "[t]he sensitivity of a particular job or access level may warrant additional background and credit checks," including for contractor employees, which should, at minimum, include character references, criminal background checks, confirmation of qualifications, and confirmation of identity. These should be supplemented, according to the FFIEC, through the use of confidentiality and non-disclosure agreements.

The Safeguards Rule establishes no similar requirements with respect to background checks on employees.[61] Particularly in smaller technology startups, where there is likely limited segregation and separation of duties, and a significant portion of the companies' small workforce may have the "keys to the castle," the lack of any requirement for background checks puts customer data at risk.

Fourth, the Interagency Guidelines and other guidance issued by the prudential regulators require banks to take an active role in overseeing the data security practices of their service providers. For example, in addition to conducting due diligence in selecting

57 See 16 C.F.R. § 314.4(c) (requiring financial institutions generally to "[d]esign and implement information safeguards to control the risks you identify through risk assessment.")

58 See 12 C.F.R. Part 30, App. B § III.C.1

59 Id. § III.A, F; IT Examination Booklet at 4-7.

60 12 C.F.R. Part 30, App. B § III.A, F.

61 See 16 C.F.R. § 314.4(a) and (b)(1).

service providers and including data security requirements in service provider contracts (both of which are generally required by the Safeguards Rule as well [62]), the Interagency Guidelines require banks, where indicated by its risk assessment, to "monitor [their] service providers to confirm that they have satisfied their obligations as required [by their contract]. As part of this monitoring, a national bank or Federal savings association should review audits, summaries of test results, or other equivalent evaluations of its service providers."[63] This requirement is supplemented by the FFIEC IT Examination Handbooks' Outsourcing Technology Services booklet, which includes an entire section on ongoing monitoring of service providers.[64] Under the Safeguards Rule, by contrast, APPs are free from express regulatory requirements mandating such ongoing vendor supervision.[65]

Fifth, guidance issued by the FFIEC regulators governing authentication requires banks to implement a risk management framework and layered security approach to prevent unauthorized activity in an online banking environment through strong authentication procedures.[66] The FTC Safeguards Rule imposes no similar specific requirement on APPs, instead only generally requiring entities subject to FTC jurisdiction to identify reasonably foreseeable risks to customer information that could result in the unauthorized use of such information, and design safeguards to control such risks. In light of this regulatory gap, it is hardly surprising that many of the APP security incidents discussed above involve authentication issues.

Sixth, the Interagency Guidelines require banks to establish an incident response program, a crucial element of data security hygiene in the increasingly dangerous threat environment. The Safeguards Rule imposes no similar requirement on APPs.

STATE LAWS AND SELF-REGULATORY STANDARDS

Neither state laws nor the PCI-DSS self-regulatory code make up for the gaps in substantive standards between the Interagency Guidelines and the Safeguards Rule.

State Laws

APPs may also be subject to general data protection or financial data security requirements under state laws, such as the Massachusetts data security regulations[67] or the Minnesota Plastic Card Security Act[68]. These laws, however, include much less detailed requirements than do the Interagency Guidelines, as supplemented by the FFIEC's IT Examination Handbook and other guidance. The Massachusetts regulations, for

62 16 C.F.R. § 314.4(d); 12 C.F.R. Part 30, App. B § III.D.1-2.

63 See12 C.F.R. Part 30, App. B § III.D.3.

64 FFIEC, Outsourcing Technology Services (June 2004), available at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_OutsourcingTechnologyServices.pdf.

65 The FTC has used its enforcement authority under Section 5 of the FTC Act (discussed below) to require ongoing monitoring of vendor data security even outside of financial institutions and the GLBA Safeguards Rule. See D. Reed Freeman, Jr. and Maury Riggan, A Primer on FTC Expectations for Your Partner and Vendor Relationships: Enforcement Shows You Are Your Brother's Keeper, Bloomberg BNA Privacy and Security Law Report 14 PVLR 781 (May 4, 2015), available at https://www.wilmerhale.com/uploadedFiles/Shared_Content/Editorial/Publications/Documents/a-primer-on-ftc-expectations-for-your-partner-and-vendor-relationships.pdf. However, for the reasons discussed below, FTC enforcement under Section 5 of the FTC Act does not compensate for specific GLBA requirements imposed on banks by prudential regulators.

66 FFIEC, Supplement to Authentication in an Internet Banking Environment.

67 Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR 17.00.

68 Minn. Stat. 325E.64.

example, which are generally regarded as the most robust state-level generally-applicable data security requirements, provide that every person that owns or licenses certain sensitive personal information about a Massachusetts resident must develop, implement, and maintain a comprehensive written information security program, and must establish and maintain a security system covering computers and any wireless system.[69] These regulations outline several topics that should be addressed in a company's information security program, including an identification and assessment of reasonably foreseeable risks; policies governing employee access to and storage of personal information; employee training requirements; and service provider oversight. While these regulations are detailed compared to other generally-applicable data security requirements, they still lack the substantial level of detail provided in the Interagency Guidelines and FFIEC guidance/IT Examination Handbook. Furthermore, while the Massachusetts Attorney General's Office is generally active in the data security field as compared to many other state Attorneys General, its resources and the weight of its enforcement actions are not comparable to a federal regulator's.

Significantly, these state laws are also generally only invoked by regulators (or by private class-action plaintiffs, in the case of some state laws providing private rights of action) *after* a problem has occurred.

69 Personal information is defined as "first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account" but does not include "information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public." 201 CMR 17.02.

Finally, even for those APP companies that require money transmitter licenses under state law, these typically fail to provide an added source of data security regulatory requirements. For example, while the New York State Department of Financial Services has been fairly active when it comes to regulating the data security of banking institutions,[70] it only requires applicants for state money transfer licenses to submit an affidavit of compliance with the *privacy* requirements of the GLBA, with no references to the data security provisions.[71] Other money transmitter license regimes say little about data security issues, focusing instead on the financial solvency of the licensees or other consumer protection concerns.[72]

Self-Regulatory Standards

APPs are potentially subject to private-sector contractual standards under the Payment Card Industry-Data Security Standards (PCI-DSS). These standards apply to entities that store, process, or transmit cardholder data and/or sensitive payment card-related authentication data (such as "track data," CVVs, or PINs). Even then, the PCI-DSS standards do not apply to entities that only process bank account data (and not payment cards), and so APPs such as Kash or Knox (which use bank accounts only) are likely exempt. PCI-DSS also applies only to

70 See, e.g., Press Release, New York State Department of Financial Services, NYDFS Issues Examination Guidance to Banks Outlining New Targeted Cyber Security Preparedness Assessments (Dec. 10, 2014), available at **http://www.dfs.ny.gov/about/press/pr1412101.htm**.

71 New York State Department of Financial Services, Instructions: Transmitter of Money License, http://www.dfs.ny.gov/banking/ialfmti.htm; Letter from Elizabeth McCaul, Superintendent of Banks, to the CEO of the Institution Addressed (Oct. 29, 2011), available at **http://www.dfs.ny.gov/legal/industry_circular/banking/il011030.htm**.

72 See, e.g., Cal. Fin. Code § 2037 (requiring California-licensed money transmitters to have a security deposit with the state Treasurer).

cardholder data environments (CDEs),[73] whereas the GLBA Interagency Guidelines, the FFIEC IT Examination Handbook, and federal banking safety and soundness requirements (discussed below) require banks to take a holistic approach to cybersecurity across their networks.

The current version of PCI-DSS includes 12 main requirements, each of which includes several sub-requirements.[74] PCI-DSS requirement 4, for example, requires covered entities to encrypt transmission of cardholder data across open, public networks.[75] This includes the following sub-requirements: (1) use strong cryptography and security protocols, including only accepting trusted keys and certificates, only supporting secure versions or configurations of the protocol in use, and using appropriate encryption strength for the encryption methodology used; (2) ensure wireless networks transmitting cardholder data or connected to the CDE use industry best practices to implement strong encryption for authentication and transmission; (3) never send unprotected payment account numbers (PANs) by end-user messaging technologies (email, instant messaging, etc.); and (4) ensure that security policies and operational procedures for encrypting transmission of cardholder data are documented, in use, and known to all affected parties.[76]

Other PCI-DSS requirements discuss encryption as well, though again with this same level of detail. Requirement 3.5, for example, mandates that covered entities document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse, including key-encrypting keys, which must be at least as strong as the data-encrypting key.[77] Standard 3.6 requires that covered entities fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including generation of strong cryptographic keys, secure cryptographic key distribution, secure cryptographic key storage, cryptographic key changes for keys that have reached the end of their cryptoperiod, retirement or replacement of keys when the key's integrity has been weakened or compromised, and prevention of unauthorized substitution of cryptographic keys.[78]

The FFIEC IT Examination Handbook's Information Security booklet includes an entire section on encryption, which goes into far more detail than PCI-DSS requirement 4 (and 3.5-3.6). For example, it provides that financial institutions should:

» employ an encryption strength sufficient to protect information from disclosure until such time as the information's disclosure poses no material threat, including by

73 Generally, a CDE refers to the network environment where cardholder data is stored, processed, or transmitting. Thus, for example, a merchant may be subject to PCI-DSS requirements in its retail environment, but if its human resources and other back-office systems are properly segregated from the retail environment, the PCI-DSS standards would not apply to this back-office environment.

74 PCI Security Standards Council, Payment Card Industry (PCI) Data Security Standard v. 3.0 (Nov. 2013), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf. The PCI Standards Security Council has also published guidance on Mobile Payment applications for developers. PCI Security Standards Council, PCI Mobile Payment Acceptance Security Guidelines for Developers (July 2014), https://www.pcisecuritystandards.org/documents/Mobile%20Payment%20Acceptance%20Security%20Guidelines%20for%20Developers%20v1%201%20.pdf.

75 PCI Security Standards Council, Payment Card Industry (PCI) Data Security Standard v. 3.0 at requirement 4.

76 Id.

77 Id. at requirement 3.5.

78 Id. at requirement 3.6.

encrypting authenticators at a strength sufficient to allow the institution time to detect and react to an authenticator theft before the attacker can decrypt the stolen authenticators;[79]

» make decisions regarding what data to encrypt and at what points to encrypt data based on the risk of disclosure and the costs and risks of encryption, but that generally, authenticators should be encrypted even on the financial institution's network, and sensitive information should be encrypted when passing over a public network and also may be encrypted within the institution;[80]

» use effective key management, which should address generating keys for different cryptographic systems and different applications, generating and obtaining public keys, distributing keys to intended users, storing keys properly, properly dealing with compromised keys, revoking keys, recovering keys that are lost or corrupted, archiving and destroying keys, logging the auditing of key management-related activities, and instituting defined activation and deactivation dates. Key management should be automated, keys should be randomly chosen from the entire key space, keys should always be encrypted using keys stored separately from the data keys, keys should be changed frequently, and should be sent securely to well-authenticated parties. Key-generating equipment should also be physically and logically secure from construction through receipt, installation, operation, and removal from service;[81]

» consider various types of encryption that may be used for different purposes, including the use of cryptographic hashes, with the addition of "salt" for passwords, secure communication protocols (like transaction layer security) for authentication, and secure shell for remote server administration;[82]

» consider encrypting data in storage, at a file, directory, volume, or disk level;[83]

» ensure "[r]obust reliability";[84] and

» employ appropriate protections for encrypted communication's endpoints.[85]

As such, even with respect to those APPs that are subject to the PCI-DSS standards, there are some significant gaps in the security requirements themselves, beyond the enforcement mechanisms or the reputational implications and risks of noncompliance.

SOME LIMITED PROGRESS

Some federal and state regulators have taken initial steps to strengthen data security requirements for APPs. The limited and preliminary nature of these steps illustrates both that regulators are beginning to recognize the substantial gaps in substantive data security requirements and that much work remains to narrow those gaps.

In June 2014, the Consumer Financial Protection Bureau (CFPB) took initial

79 FFIEC, Information Security at 52.

80 Id.

81 Id. at 52-53.

82 Id. at 54-55.

83 Id. at 55.

84 Id. at 51.

85 Id.

steps to address APP data security issues in its formal Request for Information (RFI) on the use of mobile financial products and services. The Request said that consumers are wary of data security concerns with mobile financial products, and it asked for information regarding a potential gap in security standards or risks between traditional banking channels and mobile banking, which would include APPs.[86] The FTC's response to the RFI emphasized the security concerns of mobile technologies and warned that "some industry players are not taking full advantage" of security opportunities, citing the FTC's own enforcement in the area.[87] It is not clear how the CFPB will act on the information it received in response to its request.

The CFPB has also issued informal "guiding principles" for ensuring consumer protections are built into new "faster" payment systems.[88] This one-and-a-half page document outlines nine principles, two of which implicate some of the security issues discussed in this white paper. Specifically, the guidance document provides that:

> *[T]o be safe, transparent, accessible, and efficient, faster payment systems must keep certain consumer protection concerns in mind, including the following:*
>
> *2) Data and Privacy*
> *When helpful to consumers, consumers are informed of how their data are being transferred through any new payment system, including what data are being transferred, who has access to them, how the data can be used, and potential risks. As appropriate, the systems allow consumers to specify what data can be transferred and whether third parties can access that data. When consumer data are collected, they are only used in ways that benefit consumers. The systems protect against misuse of the data associated with payment transactions.*
>
> *3) Fraud and Error Resolution Protections*
> *Faster payments are accompanied by robust consumer protections with respect to mistaken, fraudulent, unauthorized, or otherwise erroneous transactions. System architecture ensures that information is created and recorded to facilitate post-transaction evaluation. Systems provide mechanisms for reversing erroneous and unauthorized transactions quickly once identified. They also provide consumers with regulatory protections, such as Regulation E and Regulation Z, along with other appropriate safeguards.*[89]

The CFPB has thus implicitly recognized many of the concerns discussed above regarding the need for non-bank APPs to protect consumer data from misuse, prevent unauthorized transactions, and ensure consumers are reimbursed for unauthorized transactions in line with Regulation E requirements. The CFPB pledges to "work with [its] fellow regulators, entities that are developing these new [payment] systems, consumer advocates, and

86 Request for Information Regarding the Use of Mobile Financial Services by Consumers and Its Potential for Improving the Financial Lives of Economically Vulnerable Consumers, 79 Fed. Reg. 33731, 33734 (June 12, 2014). For example, the CFPB asked, in the context of economically vulnerable consumers, whether "lower cost platforms or devices carry less security and privacy protections." (Question 22(d)).

87 Comments of the Staff of the Bureau of Consumer Protection, In the Matter of Request for Information Regarding the Use of Mobile Financial services by Consumers and Its Potential for Improving the Financial Lives of Economically Vulnerable Consumers, Docket No. CFPB-2014-0012 (Sept. 10, 2014) https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-consumer-financial-protection-bureau-regarding-use-mobile-financial-services/140912mobilefinancialservices_update.pdf.

88 Consumer Financial Protection Bureau, Consumer Protection Principles: CFPB's Vision of Consumer Protection in New Faster Payment Systems (July 9, 2015), available at http://files.consumerfinance.gov/f/201507_cfpb_consumer-protection-principles.pdf.

89 Id.

other stakeholders to ensure that the new payment systems address consumer needs and interests." The guidance document, however, is non-binding.[90]

The Federal Reserve has similarly identified the need to ensure that security remains a focus in the development of faster payment systems, perhaps most formally in its January 2015 white paper, *Strategies for Improving the U.S. Payment System*.[91] In the white paper's lists of "desired outcomes," security comes second (following speed), with a goal of "U.S. payment system security that remains very strong, with public confidence that remains high, and protection and incident response that keeps pace with the rapidly evolving and expanding threat environment."[92] To achieve that outcome, the Federal Reserve lists as one of several strategies "[w]ork[ing] to reduce fraud risk and advance the safety, security and resiliency of the payment system," by establishing a payment security task force, supporting the evolution and adoption of appropriate payment security standards, expanding the Federal Reserve's anti-fraud and risk-management services, and improving the Federal Reserve's fraud data.[93] Gordon Werkema, who recently began work as full-time director of the Federal Reserve's new payment system improvement initiative, also recently noted in an interview that data security is one of his main priorities.[94] While these efforts are commendable, and show that federal financial regulators understand the security risks posed by the development of new payment technologies, these general policy efforts cannot replace meaningful regulatory requirements and oversight.

A few states have also taken initial steps into applying data security protections beyond the traditional banking context. For example, the New York State Department of Financial Services (NYDFS) included a cybersecurity requirement in its new "BitLicense" regulations covering Bitcoin and other digital currency.[95] The new rules require licensees to maintain an audited cyber security policy and program and report annually to NYDFS about the program and relevant cyber risks.[96] A proposed revision of the North Carolina Money Transmitters Act, currently pending before the North Carolina legislature, would provide the Commissioner of Banks of the State of North Carolina "the discretion to require [an] applicant [for a state money transmitter license to] obtain additional insurance coverage to address related cybersecurity risks inherent in the applicant's business model as it relates to virtual currency transmission and to the extent such risks are not within the scope" of the surety bond applicants are otherwise required to obtain.[97]

Yet even these efforts would only begin to address the gaps between banks and APPs. While the New York proposal shows NYDFS's understanding of the need to apply

90 Id.

91 United States Federal Reserve System, Strategies for Improving the U.S. Payment System (Jan. 26, 2015), available at https://fedpaymentsimprovement.org/wp-content/uploads/strategies-improving-us-payment-system.pdf.

92 Id. at 2.

93 Id. at 4.

94 Tracey Kitten, Fed's Faster Payment Security Priorities: New Director of Payments Revamp Effort Spells Out Tasks, Bank Info Security (July 14, 2015), http://www.bankinfosecurity.com/interviews/feds-faster-payments-security-priorities-i-2791#.

95 New York State Department of Financial Services, Proposed New York Codes, Rules and Regulations, Title 21, Chapter 1, Part 200, available at http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf.

96 Id. § 200.16

97 N.C. H.B. 289, § 53-208.47(d) (Mar. 19, 2015), available at http://www.ncleg.net/Sessions/2015/Bills/House/PDF/H289v1.pdf.

data security requirements to new payment technologies, these new requirements would apply only to entities engaged in digital currency businesses. Thus, they would not cover the vast majority of APPs, which do not use digital currencies. And the North Carolina proposal would not address substantive data security requirements, but would only allow the Commissioner the discretion to require the entity to mitigate the *financial* risks of a cybersecurity incident to the company, rather than the *consumer* risks.

IV. APPs are Not Subject to Meaningful Oversight or Enforcement to Prevent Breaches Before They Harm Consumers

Not only do APPs face less stringent data security standards than do banks, but as a practical matter they are likely to face sanctions for lax data security practices only if they suffer an actual cybersecurity breach that becomes known to the government. That is because banks, unlike APPs, are subject to regular examinations, enforcement actions, and other oversight by prudential regulators. As in the regulatory context discussed above, the FTC lacks the authority and resources to provide a sufficiently robust parallel to the examination and enforcement regime administered by the financial regulators.

EXAMINATION

Unlike banks, APPs are not subject to meaningful data security examination, in which a regulator could scrutinize an APP's data security practices in order to identify and correct weaknesses before they are exploited by an attacker. Even as to those APPs that are "financial institutions" subject to the FTC's Safeguards Rule (and therefore subject to possible FTC enforcement under the Rule), the FTC does not exercise examination authority. Instead, it can only target individual APPs using its Civil Investigative Demand (CID) process, similar to a subpoena. Targeted, one-off CIDs hardly compare to broad and frequent examinations, in which financial examiners have the right to routinely review evidence of compliance if the target falls within its supervisory jurisdiction. The FTC also has limited resources, which preclude it, as a practical matter, from covering all APPs (and all the other companies in other sectors subject to its jurisdiction). While the FTC has, in recent years, taken an increased interest in the financial technology, or "FinTech," industry in general,[98] few of these efforts have been targeted at security-related issues, and have instead focused primarily on issues regarding deceptiveness, advertising law violations, and consumer privacy.

At present APPs are not subject to CFPB examination authority either. The CFPB has examination authority over nonbanks only to the extent the nonbanks are mortgage lenders or services, student or payday lenders, or have been identified via rulemaking as "larger participant[s]" in markets for consumer financial products or services.[99] The CFPB has not issued a rule identifying "larger participants" in the payments market. Even if there were such a rule, most APPs would likely, by virtue of their size, not be covered. The smaller APPs are the ones most likely to lack adequate data security or privacy safeguards, despite dealing in highly sensitive consumer financial data as a core function of its business.[100]

98 See, e.g., Federal Trade Commission, Financial Technology: Protecting Consumers on the Cutting Edge of Financial Transactions, https://www.ftc.gov/news-events/media-resources/consumer-finance/financial-technology.

99 12 U.S.C. § 5514(a)(1)(B), (b).

100 Financial regulators have expressly recognized this risk. In the Winter 2012 edition of the Federal Deposit Insurance Corporation (FDIC) publication "Supervisory Insights," the FDIC

Some APPs may be licensed state money transmitters or federally-registered money services businesses (MSBs), and would therefore be subject to state and/or Internal Revenue Service (IRS) examinations. But these examinations are not comparable to the sophisticated, in-depth examinations carried out by federal prudential regulators guided by the FFIEC IT Exam Handbook. IRS examiners are focused primarily on anti-money laundering, not data security, and rarely conduct examinations outside of major money transmitters due to staffing and resource constraints. State examinations similarly do not occur on a regular basis, and, even when they do occur, as a practical matter pale in comparison to federal examinations. By contrast, large banks and other FFIEC-examined financial institutions are examined consistently. Without a realistic threat of consistent and sophisticated data security examination, APPs face a low risk of being caught in a state of non-compliance until it is too late and customers may have suffered harm through fraud and/or unauthorized access to their sensitive personal or financial information.

The lack of meaningful examination authority with respect to these entities has significant consequences with respect to data security and regulatory burdens.

First, because APPs are not regularly examined, it is easier for their security flaws to go undetected, unless they ultimately lead to a breach resulting in a sufficiently high amount of fraud such as to trigger detection by the card brands and/or banks (or they self-detect). In general, the FTC tends not to launch data security investigations and/or bring enforcement actions against companies unless some event has brought the issue to the FTC's attention (such as a data breach, whistleblower complaint, or public reporting on a security flaw).[101]

noted that financial institutions should have a review and approval process for new mobile payment product offerings that ensures compliance with internal policies and applicable laws, a process that is particularly challenging because "much of the innovation in the mobile payments marketplace is driven by entrepreneurial companies that may not be familiar with supervisory expectations that apply to banks and their service providers." FDIC, Mobile Payments: An Evolving Landscape (Winter 2012), available at **https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin12/mobile.html** (emphasis added). In other words, here too, the onus is on banks to exercise their authority over service providers when partnering with mobile payment providers to make sure those providers understand the examination authorities' requirements. This ignores the fact that those APPs not functioning as bank service providers are particularly high risk, as they are completely immune from supervisory authority while also lacking the financial institution partner to mentor them through (and likely bear the cost of) compliance and appropriate implementation of supervisory expectations. See also Susan Pandy, Update on the U.S. Regulatory Landscape for Mobile Payments, Summary of Meeting between Mobile Payments Industry Workgroup (MPIW) and Federal and State Regulators at 2 ("A guiding principle of the Mobile Payments Industry Workgroup (MPIW) is the need for a common understanding of the regulatory environment for the mobile payments industry. Key concerns relate to . . . how knowledgeable alternative payment providers are, particularly start-ups, with banking laws for consumer protection and privacy, . . . data security, . . . and risk compliance . . .").

101 For example, a review of the approximately 13 cases in which the FTC has brought enforcement actions for violations of the Safeguards Rule reveals that:

- eight involved breaches (including six cases where personal information was clearly breached and two cases where breaches occurred that could have allowed access to personal information, but where the complaint does not make clear whether such information was actually accessed); In the Matter of Franklin's Budget Car Sales, Inc., also d/b/a Franklin Toyota/Scion, FTC Matter/File No. 102 3094 (Oct. 26, 2012); In the Matter of ACRAnet Inc., FTC Matter/File No. 092 3088 (Aug. 19, 2011); In the Matter of Fajilan and Assocs., Inc., also d/b/a Statewide Credit Servs., FTC Matter/File No. 092 3089 (Aug. 19, 2011); In the Matter of SettlementOne Credit Corp. and Sackett Nat'l Holdings, Inc., FTC Matter/File No. 082 3208 (Aug. 19, 2011); In the Matter of James B Nutter & Co., FTC Matter/File No. 072 3108 (June 16, 2009); In the Matter of Premier Capital Lending, Inc., et al., FTC Matter/File No. 0723004, Docket Number C-4241 (Dec. 16, 2008); In the Matter of Goal Fin., LLC, FTC Matter/File No. 072-3013 (Apr. 15, 2008); In the Matter of Nations Title Agency, Inc., et al., FTC Matter/File No. 052 3117 (June 20, 2006).
- two involved violations of the "Disposal Rule" under the Fair

Perhaps because of this, APPs may also be less likely to report breaches unless they have no other alternative. While the FTC has generally viewed an incident response plan as part of a reasonable and appropriate data security program in exercising its FTC Act Section 5 authority,[102] no federal regulation expressly requires APPs to have an incident response plan. They are thus unlike banks, which are required to have such a plan under the Interagency Guidelines. While many breaches involving personal information held by APPs may trigger state data breach notification laws, the triggering of the notification requirement will turn on the precise information disclosed or accessed.

Second, beyond formal law or guidance, banks are often subject to expectations by their prudential regulators that as a practical matter they must follow. Thus, banks may have better privacy/data security standards, or better treatment because their regulators will ask for it, and these standards may not be shared by APPs. For example, in a related context, most (if not all) major banks will waive consumer liability for unauthorized ACH transactions (*e.g.*, ACH withdrawals conducted by an attacker who has stolen personal information), as long as the consumer reports them in a reasonable amount of time. Regulation E, however, allows the institutions to place up to $500 liability on the consumer if the consumer does not provide timely notice.[103]

As a preliminary matter, it is unclear whether APPs are subject to Regulation E, as its terms might not technically apply to APPs.[104] This would mean that consumers will not have the statutory and regulatory protections of Regulation E for these services, though some APPs may provide such protections on a voluntary basis. Even when Regulation E does apply, banks often feel compelled to waive even the $500 liability allowed under Regulation E because of their regulator's expectations, whereas APPs may choose to provide liability protection only consistent with Regulation E's requirements (whether because they are covered by Regulation E or on a voluntary basis).

and Accurate Credit Transactions Act, 16 C.F.R. Part 682 (with violations of the Safeguards Rule being charged as a secondary count). U.S. v. PLS Fin. Servs., Inc. et al., FTC Matter/File No. 1023172, No. 112-cv-08334 (Nov. 7, 2012); U.S. v. Am. United Mortg. Co., FTC Matter/File No. 062 3103, 07C 7064 (Dec. 18, 2007).

three cases, all from the 2004-2005 period, which were the first three enforcement actions brought by the FTC under the Safeguards Rule, resulted from general sweeps conducted against a specific industry: mortgage lenders. In the Matter of Superior Mortg., FTC Matter/File No. 052 3136 (Dec. 16, 2005); In the Matter of Nationwide Mortg. Grp., Inc. et al., FTC Matter/File No. 042-3104, 9319 (Apr. 15, 2004); In the Matter of Sunbelt Lending Servs., FTC Matter/File No. 042 3153 (Jan. 7, 2005). In general, the FTC does not tend to conduct general Section 5 sweeps on data security matters.

102 See e.g., In the Matter of EPN Inc., FTC Matter/File No. 112-3143 (Oct. 26, 2012).

103 12 C.F.R. § 205.6.

104 In general, Regulation E provides protections with respect to "electronic fund transfers," defined as "any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account." 12 C.F.R. § 1005.3(b)(1). Currently, "account" is defined to mean "a demand deposit (checking), savings, or other consumer asset account (other than an occasional or incidental credit balance in a credit plan) held directly or indirectly by a financial institution and established primarily for personal, family or household purposes." Id. § 1005.2(b). Although consumers may use traditional payment systems to prefund the "payment accounts" in P2P or other APP platforms (e.g., through a debit card transaction or an ACH transfer from a bank account) and would thus receive protection under Regulation E for certain transfers to the payment account, it is unclear whether Regulation E applies to P2P transfers made from the "payment account," given that these stored value accounts are not explicitly covered by Regulation E's existing definition of "account." That said, this may change for certain APPs if the CFPB's proposed prepaid rule is finalized as written. See , Prepaid Accounts under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z), 79 Fed. Reg. 77,101 (Dec. 23, 2014), as amended by Prepaid Accounts under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z), 80 Fed. Reg. 6,468 (Feb. 5, 2015).

Here, again, APPs freedom from examination by a federal regulator means that consumers enjoy less protections when using an APP than when getting the same service from a bank.

There is at least some evidence that some APPs in this context do provide less consumer protection than banks. For example, according to Venmo's user agreement, if a user believes that their account registration information, PIN, or mobile device has been lost or stolen, and the account history shows unauthorized transactions, users who contact Venmo within two business days after learning of the loss or theft will only be liable up to $50, while liability for losses reported later will not exceed $500.[105] While it is possible that, as a matter of practice, Venmo may refund the entire transaction, it is hard to tell based on coverage of Venmo's issues with fraud. Because Venmo lacks the full-time customer service staff that a large bank provides, the article discussed above notes that the unauthorized withdrawal was refunded by the user's bank by the morning after he reported it, while Venmo took that long to even respond to his inquiries. This tactic might even be an intentional one by APPs; because they know the customers will quickly reach out to their banks and banks will make them whole (or face potential regulatory liability for failing to do so), they may intentionally lack a system in place to quickly address and resolve unauthorized transactions. And, notably, other APPs not subject to Regulation E disclaim any liability whatsoever, or otherwise provide less protection than the protection banks are required to provide by Regulation E.[106]

Finally, even where there is overlap between the GLBA requirements imposed by prudential regulators and the PCI-DSS requirements, the manner in which these standards are enforced varies substantially (even beyond the fact that PCI-DSS is a private sector standard rather than a standard enforceable through government examinations and enforcement).

105 Venmo U.S. User Agreement, Sections C.1.n.iv, E.9, **https://venmo.com/legal/us-user-agreement/**; Allison Griswold, Venmo Money, Venmo Problems, Slate (May 14, 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** ("After two business days, your liability can jump as high as $500, per Venmo's terms."). See also LevelUp, User Terms of Service, Section 6, **https://www.thelevelup.com/terms** (noting that LevelUp will reimburse all fraudulent or unauthorized transactions made using the LevelUp user account if reported within two days of the first transaction (or loss of device), providing no coverage for activities not reported within 60 days, and providing up to $500 of coverage for notices provided after two business days).

106 See, e.g., Square, Square Wallet User Agreement, **https://squareup.com/legal/pay-ua** at ¶ 15 ("Security. We have implemented technical and organizational measures designed to secure your personal information from accidental loss and from unauthorized access, use, alteration or disclosure. However, we cannot guarantee that unauthorized third parties will never be able to defeat those measures or use your personal information for improper purposes. You acknowledge that you provide your personal information at your own risk."); ¶ 25 (Limitation of Liability and Damages. . . . UNDER NO CIRCUMSTANCES WILL SQUARE BE RESPONSIBLE FOR ANY DAMAGE, LOSS, OR INJURY RESULTING FROM HACKING, TAMPERING, OR OTHER UNAUTHORIZED ACCESS OR USE OF SQUARE WALLET, YOUR SQUARE WALLET ACCOUNT, OR THE INFORMATION CONTAINED THEREIN."); Square, Square Cash Agreement (Mar. 23, 2015), **https://squareup.com/legal/cash-ua** (containing similar limitation of liability language, though not including the same security language); Kash, User Agreement, **https://withkash.com/user_agreement.html** ("If you believe that any of your Kash App, account registration information, PIN or mobile device containing the Kash App has been lost or stolen, or if your account history shows transfers that you did not make, you must immediately contact Company via the Contact Us information below or by email to **legal@withkash.com**. If you contact Company within one Business Days after learning of the loss or theft, then your liability shall not exceed the lesser of $75.00 USD or the amount of unauthorized transfers that took place on your account before you provided notice to Company. If you do not contact Company within one Business Days of learning of the loss or theft, then your liability shall not exceed the lesser of (a) $1000.00 USD or (b) the sum of (i) the lesser of $75.00 USD or the amount of unauthorized transfers that occur within one Business Days of learning of the loss and (ii) the amount of unauthorized transfers that occur after the close of one Business Days and before notice to Company, provided that Company can establish that the expenditures would not have occurred had you notified Company within one Business Days of the loss.").

Under PCI-DSS, covered entities are required to undergo regular (usually, annual) assessments by certified PCI Qualified Security Assessors, which result in the completion of a Report on Compliance (ROC). While this may sound like the private sector equivalent of a regulator examination, it is far less rigorous. PCI-DSS audits are generally paper audits, and ROCs rarely conclude a lack of compliance, thereby allowing the vast majority of PCI-DSS covered entities to make claims about being certified as PCI-DSS compliant. With many of the more recent retail breaches, companies have been allegedly PCI-DSS compliant according to their most recent ROC, but the post-breach forensic review finds several violations of PCI-DSS.[107]

As such, even where an entity is certified as PCI-DSS compliant, this does not actually mean that they are, in fact, compliant with the PCI-DSS standards or that their networks are truly secure. In other words, to the extent the PCI-DSS review process has teeth, it is only *after* a breach has already occurred – much the same as with the FTC GLBA Safeguards Rule and FTC Act authority (discussed below). In contrast, the examination procedure is intended to ensure that banks have proper security processes in place to *prevent* a breach – and the risks of failing an examination provide significant incentive for banks to expend significant capital to ensure compliance. By contrast, the risk of failing a PCI-DSS assessment prior to a breach is low and, even where noncompliance is found, monetary fines are relatively minimal – *e.g.*, tens of thousands of dollars per card network – compared to the cost of regulatory fines. And a card brand fine, which may not even be public, pales in comparison from a reputational standpoint to a publicized federal regulator enforcement action.

107 See, e.g., Jaikumar Vijayan, After Target, Neiman Marcus breaches, does PCI compliance mean anything?, ComputerWorld (Jan. 24, 2014), http://www.computerworld.com/article/2486879/data-security/after-target--neiman-marcus-breaches--does-pci-compliance-mean-anything-.html.

ENFORCEMENT

Gramm-Leach-Bliley Act

The GLBA delegates enforcement of its data security provisions to the federal banking agencies with respect to banks and to the FTC with respect to the kinds of financial institutions that include APPs.[108] While both banks and APPs may be subject to injunctive relief for violations of the GLBA's requirements,[109] only banks face a realistic possibility of civil money penalties. Under the federal banking laws, a bank's prudential regulator can assess civil money penalties if the bank "violates any law or regulation," including GLBA and the Interagency Guidelines.[110] The penalties are significant. Banks might be fined $7,500 per violation per day, or as much as $37,500 per violation per day if the regulator determines that the violation is part of a "pattern of misconduct."[111] By contrast, the FTC cannot assess civil penalties at all if an APP violates the Safeguards Rules. The FTC is limited to getting injunctive relief. APPs are subject to civil penalties only if they violate an existing final order by the FTC, and only if the FTC can convince the Department of Justice to bring suit to collect the penalties.[112] APPs must thus commit the same violation twice before they can be penalized. Penalties are capped at $16,000 per violation.[113]

108 15 U.S.C. § 6805(a).

109 See 12 U.S.C. § 1818(b) (equitable relief under the banking laws); 15 U.S.C. 53(b) (equitable relief under the FTC Act).

110 12 U.S.C. § 1818(i).

111 Id. (adjusted for inflation by 77 Fed. Reg. 66529 (Nov. 6, 2012)).

112 15 U.S.C. § 45(l).

113 Id.

The FTC's lack of penalty authority creates vastly different consequences for banks and nonbanks for violations of the same statute.[114] While both the FTC and banking agencies have restitution authority, showing customer harm for data security failures is difficult, especially where no breach can be proven. In fact, the FTC's GLBA data security settlements to date have not obtained any monetary relief for consumers for such GLBA violations.[115] Without the threat of civil penalties, APPs are unlikely to suffer direct monetary loss for data security lapses, which in turn provides less incentive for them to meet Safeguards Rule requirements.

Unfair, Deceptive (and Abusive) Acts or Practices

APPs, like most companies, are presumably subject to the FTC's jurisdiction under Section 5 of the FTC Act, which prohibits companies from engaging in unfair or deceptive acts or practices (UDAP) in or affecting interstate commerce.[116] The FTC has, in recent years, used this authority to bring enforcement actions against companies across the economy with respect to "unfair" data security practices.[117] However, the general threat of a UDAP enforcement action for failure to satisfy a vague concept of "reasonable and appropriate" information security practices does not compensate for the otherwise insufficient data security requirements that govern the practices of APPs, for several reasons.

First, banks subject to the Interagency Guidelines are also subject to FTC Act UDAP enforcement by their prudential regulators.[118] Banks (and some APPs) may also be subject to similar restrictions by the CFPB (which has authority to bring enforcement actions against banks and other covered financial institutions for engaging in unfair, deceptive, or abusive acts or practices, or UDAAP). While the CFPB has yet to bring a public enforcement action under its UDAAP authority for data security, it is at least possible, if not likely, that the CFPB will begin to move into this space as the relatively new Bureau matures as an agency.[119] However,

114 The FTC can enforce GLBA violations administratively or in federal district court, while the banking agencies can only pursue administrative relief. The option of proceeding in court has little practical impact, however, because the FTC faces a lower burden in administrative proceedings, where it "has the first opportunity to make factual findings and articulate the relevant legal standard," and the court must affirm findings of fact if supported by substantial evidence. Thus, "where a case involves novel legal issues or fact patterns, the Commission has tended to prefer administrative adjudication." FTC, A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority (Jul. 2008), available at **https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority**.

115 See, e.g., U.S. v. PLS Fin. Servs., Inc. et al., FTC Matter/File No. 1023172, No. 112-cv-08334 (Nov. 7, 2012) (alleging both FCRA and GLBA violations, but assessing monetary penalties only with respect to the FCRA violations, and requiring comprehensive information security programs and assessments, but not awarding restitution or other monetary relief with respect to the alleged GLBA violations); U.S. v. Am. United Mortg. Co., FTC Matter/File No. 062 3103, 07C 7064 (Dec. 18, 2007) (similarly assessing monetary penalties only for alleged FCRA violations and not alleged GLBA violations); In the Matter of Franklin's Budget Car Sales, Inc., also d/b/a Franklin Toyota/Scion, FTC Matter/File No. 102 3094 (Oct. 26, 2012) (barring misrepresentations regarding data security and requiring comprehensive information security programs, but not awarding restitution or other monetary relief).

116 15 U.S.C. § 45(a)(10).

117 See Federal Trade Commission, 2014 Privacy and Data Security Update, **https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf**.

118 See, e.g., In re Bancorp Bank, FDIC 11-698b & 11-703k (Aug. 12, 2012) (consent order and civil money penalty for violations of the FTC Act); see Julie L. Williams, First Sr. Deputy Comptroller and Chief Counsel, Office of the Comptroller of the Currency, Remarks at the Mid-Atlantic Bank Compliance Conference (Mar. 22, 2002), available at **http://www.occ.gov/static/news-issuances/speeches/2002/pub-speech-2002-30.pdf**. ("When a bank's marketing practices cross the line from being bad customer relations to become unfair or deceptive practices [violating the FTC Act], the OCC (and the other federal banking agencies) have authority to intervene.").

119 See Jonathan Cedarbaum and Elijah Alper, The Consumer Financial Protection Bureau as a Privacy & Data Security Regulator, FinTech Law Report Vol. 17 Iss. 3 at 2 (May/Jun. 2014), available at **https://www.wilmerhale.com/**

banks are *also* subject to the general UDAP/UDAAP restrictions on top of the specific GLBA data security requirements imposed by the Interagency Guidelines and accompanying prudential regulator/FFIEC guidance. The potential applicability of this UDAP/UDAAP authority to regulate APP's data security thus does nothing to level the uneven playing field caused by the two different GLBA regimes.

Second, FTC enforcement of data security standards for financial institutions under its UDAP jurisdiction has not been particularly robust, and has generally been used only to add additional charges in enforcement actions already being brought under the Safeguards Rule.[120]

Third, both the FTC's and CFPB's prohibitions on unfair practices require a likelihood of substantial injury that cannot be reasonably avoided by consumers.[121] No such finding is required for a violation of the Interagency Guidelines or accompanying guidance.

Fourth, the FTC's authority to regulate data security through its unfairness authority is currently subject to a forceful challenge in the *Wyndham* case, currently pending before the Third Circuit.[122] Should Wyndham prevail, there would be even less oversight of APPs' data security practices.

In addition to "unfairness" claims under the FTC Act Section 5's UDAP prohibition, APPs are subject to the UDAP prohibition on deceptive practices. As with the unfairness prong of Section 5 noted above, the deceptiveness prohibition applies to banks as well.[123] The odds of the FTC's bringing a deceptiveness claim against an APP over data security, though, in the absence of a publicly disclosed breach, a whistleblower tip, or evidence produced in response to a targeted CID, are much lower than a bank regulator, with constant supervisory access to bank records, bringing a similar claim against a bank. This may allow APPs to make general and untested statements about their security—such as claiming to use "bank grade security,"[124] to be "100% compliant to the letter and intent of all PCI regulations, rules and recommendations,"[125] to have security teams "work[ing] day in and day out to ensure [the APP is] . . . the safest way to pay,"[126] to "stop[] fraud before it happens,"[127] and to be "not just a payments company, [but] a security company"[128] —without the degree of regulatory scrutiny that banks would face for similar statements.

DATA SECURITY VIA SAFETY AND SOUNDNESS REGULATION

In addition to data security-specific enforcement

uploadedFiles/Shared_Content/Editorial/Publications/Documents/fintech-law-report-CFPB-privacy-date-security-regulator-may-june-2014.pdf.

120 See, e.g., In the Matter of Fajilan and Assocs., Inc., also d/b/a Statewide Credit Servs., FTC Matter/File No. 092 3089; In the Matter of SettlementOne Credit Corp. and Sackett Nat'l Holdings, Inc., FTC Matter/File No. 082 3208 (both charging violations of the GLBA Safeguards Rule, the Fair Credit Reporting Act, and the FTC Act).

121 15 USC 45(a); 12 USC 5531(a).

122 FTC v. Wyndham Worldwide Corp. et al., 212-cv-01365-SPL. The FTC's authority is also being challenged in enforcement action brought against LabMD, though it is still in the administrative stage and has not yet been moved to an Article III court. In the Matter of LabMD, Inc., FTC Matter/File no. 102 3099 (2015).

123 See n.105.

124 Venmo, Security, https://venmo.com/about/security/.

125 LevelUp, Our Commitment to Security, https://www.thelevelup.com/security.

126 Id.

127 Square, Security, https://squareup.com/security.

128 Knox Payments, Features, https://knoxpayments.com/features.

and oversight, banks face an additional federal requirement—safety and soundness regulation—under which regulators can hold them accountable for substandard data security programs *even if no breach and no harm occurs*. By contrast, as discussed above, APPs and other nonbanks are subject only to a less rigorous implementation of the GLBA data security standards and the FTC's enforcement of UDAP (and CFPB's enforcement of UDAAP), assuming they survive the *Wyndham* challenge. Here too, then, the regulatory playing field is tilted in favor of APPs and against consumers entrusting their private data to those companies.

Banks are uniquely subject to federal safety and soundness regulation, which requires banks to avoid whatever their regulators deem to be "unsafe or unsound practices."[129] Federal courts have articulated a number of tests for unsafe or unsound practices. The D.C. Circuit has held that an "unsafe or unsound practice" is one that poses "a reasonably foreseeable undue risk to a banking institution."[130] The OCC has stated that this articulation is consistent with its own standard, which is that an unsafe or unsound practice is any action "contrary to generally accepted standards of prudent operation, the possible consequences of which, if continued, would be abnormal risk or loss or damage to an institution, its shareholders, or the agencies administering the insurance funds."[131]

Any bank offering insured deposits that engages in "unsafe or unsound practices" is subject to a cease and desist order from the bank's prudential regulator.[132] The consequences of engaging in such practices are steep. The order can include virtually any equitable remedy, including indemnification to other parties, restitution to customers, rescission of contracts, disposal of assets or, any other action the regulator "determines to be appropriate."[133] And if a bank is found to have "recklessly" engaged in such practices,[134] the agency may assess severe civil monetary penalties. In the past year alone, the federal banking agencies have assessed nine civil penalties of more than $40 million each, not because a bank violated any substantive law,

129 Several states examine money transmitters for safety and soundness. See, e.g., Ohio Rev. Code § 1315.12(a)(2); Ariz. Dep't of Fin. Inst., Money Transmitters, at http://www.azdfi.gov/Licensing/Licensing-FinServ/MT/MT.html (last visited [date]) ("It is the policy of AZDFI to select the most effective and efficient methods of conducting examinations so that significant risks affecting safety and soundness, as well as substantive statutory compliance, can be identified and, if necessary, appropriate supervisory action taken."). However, many APPs, such as Apple Pay, take the position that they are not subject to state or federal money transmitter license requirements. See, Wall. St. Journal, Apple Pay Faces Lighter Compliance than Paypal, Google (Oct. 20, 2014), available at http://blogs.wsj.com/riskandcompliance/2014/10/20/why-apple-pay-faces-lighter-compliance-than-paypal-google/). Also, we understand that safety and soundness examinations focus on the insolvency of money transmitters. See, e.g., Tex. Code § 151.301(b)(9) ("'Unsafe or unsound act or practice' means a practice of or conduct by a license holder or an authorized delegate of the license holder that creates the likelihood of material loss, insolvency, or dissipation of the license holder's assets, or that otherwise materially prejudices the interests of the license holder or the license holder's customers."). We are not aware of state regulators [consistently] assessing civil penalties for practices deemed unsafe and unsound but unrelated to licensee solvency.

130 Dodge v. Comptroller of Currency, 744 F.3d 148, 155 (D.C. Cir. 2014).

131 See In the Matter of Patrick Adams, OCC AA-EC-11-50 (Sept. 30, 2014).

132 12 USC 1818(b). Typically, banks enter into consent orders, which are settlement agreements based on the regulators' cease and desist authority. The reputational and financial risks of litigating against a banking regulator are so large that no major bank this century has refused to settle a pending enforcement action. The reluctance to litigate allows regulators to push the limits of their cease and desist authority or their interpretations of what constitutes an unsafe or unsound practice.

133 12 USC 1818(b)(6).

134 To meet the "reckless" standard, a bank must have engaged in conduct "in disregard of, and evidencing conscious indifference to, a known or obvious risk of a substantial harm." Cavallari v. OCC, 57 F.3d 137, 142 (2d Cir. 1995). The OCC has said that a bank's conduct is reckless if the bank evidences disregard of, or indifference to, the consequences of the practice, even though no harm may be intended. See OCC PPM 5000-7, App'x C, at C-4.

but merely the bank's practices were not "safe and sound."[135]

As noted above, the FTC's and CFPB's prohibitions on unfair practices require a likelihood of substantial injury that cannot reasonably be avoided by consumers.[136] A bank, however, may engage in "unsafe or unsound practices" without any injury occurring or likely occurring at all to consumers. Rather, all that is required is that a bank's actions be deemed contrary to "standards of prudent operation," *i.e.*, that they not meet accepted regulatory standards. Thus, a bank with a data security system that does not meet the Interagency Guidelines, or one that does meet those guidelines but is otherwise deemed insufficient by regulators, may face public enforcement and large penalties even if no breach occurs and even if not a single consumer is harmed or is likely to be harmed.

The application of safety and soundness principles to data security standards is not merely theoretical. In 2013, the FDIC and OCC entered into a joint consent order against two bank technology service providers based on unsafe and unsound practices relating to data security. According to the two regulators, the service providers committed unsafe or unsound practices by, among other things: operating without certain procedures to "identify and address software vulnerabilities" and without certain programs to "detect, identify and act on potential threats in a timely manner."[137] Nor can banks avoid liability by outsourcing data protection to such vendors; regulators have repeatedly held banks liable for failures by their service providers.[138] Thus, banks are essentially required to maintain sound data protection systems that meet whatever criteria the regulators deem consistent with "generally accepted standards of prudent operation."

APPs, by contrast, operate free of any federal safety and soundness requirements. Because they face no federal liability simply for unsafe or unsound practices, in practice they cannot be held liable for even the most reckless data security standards unless or until a breach occurs.

135 See, e.g., In re Bank of America, N.A. No. AA-EC-14-99 (Nov. 11, 2014) (assessing $250 million civil money penalty for unsafe or unsound practices relating to foreign exchange transactions, without alleging a violation of law); OCC Release No. NR-2012-20 (Feb. 9, 2012) announcing $404 million in civil money penalties against four banks for unsafe and unsound mortgage practices, without alleging a violation of law).

136 15 USC 45(a); 12 USC 5531(a).

137 See In re FUNDtech Corp. & BServ, Inc., FDIC-13-0452b,OCC-AA-NE-2013-106 (Dec. 5, 2013).

138 For example, the series of orders against major banks regarding the marketing and servicing of credit card add-on products are based primarily on conduct by the banks' service providers. See, e.g., In re Bank of America, N.A., 2014-CFPB-004 (Apr. 9, 2014) at ¶ 17 (alleging improper conduct based on actions by bank "through its Service Providers").

V. Costs Remain with the Banks for APPs' Lapses

The uneven data security playing field between banks and APPs not only has real consequences with respect to the potential for consumer harm and the uneven burden placed on financial institutions with respect to regulatory compliance. It also manifests itself with respect to which entities bear the brunt of costs in the wake of a data security compromise of an APP. Here, too, banks are likely to be left with the bill. In the event that a customer's payment card or bank account data is stolen from an APP, resulting in fraudulent charges, banks are often, at least in the first instance, paying the costs. This includes not only refunding unauthorized transactions (which could be substantial in themselves), but also the cost of replacing cards and/or closing accounts, as well as the administrative costs of identifying relevant cards/accounts and increased fraud detection efforts. To the extent any of these fees would be recoverable from the APPs in the event of a breach involving APP data, this would likely only be indirectly through litigation and/or PCI-DSS enforcement fines by the card brands.

Even when APPs are in theory responsible for directly reimbursing consumers for unauthorized transactions that occur on their platforms when APP accounts themselves are compromised, customers are still likely to turn to their banks where their banks are more responsive to customer inquiries. That was the case at least in the instance described by the article on Venmo, where Chase reportedly made the customer whole.[139] And even if the APP did reimburse the fraudulent charge, the banks are still the ones left with the administrative hassle on the backend to close the account and reissue cards.

139 Allison Griswold, Venmo Money, Venmo Problems, Slate (May 14, 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.

VI. Recommendations

Banks and APPs engaging in functionally similar activities should be subejct to similar regulatory regimes. A regulatory level playing field of this sort is critical both to ensure that consumers enjoy consistent protection regardless of their choice of platform and to protect the safety and soundness of payment systems. To close the regulatory, enforcement, and examination gaps that exist today, we recommend the actions set forth below.

NON-LEGISLATIVE

Many of the legal and regulatory disparities noted above could be remedied through federal and state regulation that treats APPs and banks similarly with respect to data security issues. As noted above, the CFPB and a few states have begun to acknowledge or address security concerns of some APPs, though these efforts illustrate just how wide the gap remains between the industries. Much more remains to be done, including:

» *Enhancing the substantive regulatory requirements.* Because the substantive scope of the FTC's statutory authority under the GLBA is the same as that of the prudential regulators, the FTC should adopt enhanced GLBA Safeguards Rules, either limited to APPs (in which case this term would have to be defined in a way to sufficiently address both current and future participants in this industry) or applicable more broadly to all companies subject to the FTC's jurisdiction.

» Using available examination authority.

- The CFPB should issue rules defining larger participants of the APP industry, which would give the CFPB examination authority over those larger participants as defined; and

- To the extent the CFPB or another regulator has authority to examine APPs that are established as service providers of a financial institution subject to its examination jurisdiction, it should exercise such authority.

» Enforcing existing requirements.

- The FTC should enforce its GLBA Safeguards Rule more frequently for APPs, perhaps including through a CID sweep; and

- For APPs federally registered as money services businesses with the Financial Crimes and Enforcement Network (FinCEN), FinCEN should enforce existing guidance suggesting that financial institutions report actual or attempted data breaches to the government in the form of suspicious activity reports (SARs), just as it does for banks.[140]

  Doing so would force registered APPs to monitor for such breaches and encourage them to take steps to bolster their cybersecurity practices.

LEGISLATIVE

In some cases, legislation may be the best method of ensuring consistent data security standards by either (1) closing the regulatory

140 See, e.g., Account Takeover Activity, FIN-2011-A016 (Dec. 19, 2011), available at http://www.fincen.gov/statutes_regs/guidance/html/FIN-2011-A016.html.

and enforcement gap by establishing comprehensive and cross-industry data security requirements, or (2) closing the regulatory, examination, and enforcement gaps by giving financial regulators authority over the data security practices of APPs in particular. Some of the data breach notification bills pending in Congress fall into that first group by including provisions that would provide the FTC with broad rulemaking authority over data security,[141] while others would give the FTC express enforcement authority over either general or specific data security requirements included in the bills.[142]

An example in the second category is the Data Security Act of 2015 (S. 961 and H.R. 2205), which would establish a flexible process for firms of all sizes that handle consumers' sensitive financial information to follow in order to secure data and prevent breaches. These standards are based on the GLBA Interagency Guidelines, and would result in common-sense standards that have already proven flexible enough to work effectively for both large and small financial institutions, and can thus effectively be applied to APPs of all sizes. While many of the security requirements included in Data Security Act are similar to the FTC Safeguards Rule, the Data Security Act includes a few additional requirements that could help level the playing field between banks and companies not subject to the GLBA. These include:

» a requirement to "reasonably oversee or obtain an assessment of [a] service provider's compliance with contractual [data security] obligations, where appropriate in light of the covered entity's risk assessment;"[143]

» mandating that covered entities "consider whether [various] security measures are appropriate for the covered entity and, if so, adopt those measures that the covered entity concludes are appropriate," including access controls, physical access restrictions, encryption of electronic information in transit or in storage, procedures to ensure that information system modifications are consistent with the covered entity's information security program; dual control procedures, segregation of duties, and employee background checks for employees with access to sensitive information; monitoring systems and procedures to detect actual and attempted attacks on, or

141 See, e.g., Consumer Privacy Protection Act of 2015, S. 1158, 114th Cong. (2015) Subtitle A (requiring covered entities to comply with safeguards designated in the Act and any other administrative, technical, or physical safeguards identified by FTC through rulemaking, providing FTC with enforcement authority for violations of those requirements, and defining a violation of those requirements as an unfair or deceptive act or practice under the FTC's Section 5 authorities); Data Security and Breach Notification Act of 2015, S. 177, 114th Cong. (2015) § 2 (directing FTC to promulgate regulations to require each covered entity that owns or possesses data containing personal information, or contracts to have a third-party entity maintain or process data on its behalf, to establish and implement policies and procedures regarding information security practices for the treatment and protection of personal information) and § 5(c) (providing that a violation of § 2 shall be treated as an unfair and deceptive act or practice in violation of a regulation issued under the FTC's Section 5 authority, and subject to FTC enforcement).

142 See, e.g., Data Security Act of 2015, H.R. 2205, 114th Cong. (2015) § 4(a) (requiring companies to develop, implement, and maintain a comprehensive information security program, with specifically listed elements and security controls) and § 5(a)(9) (providing FTC with authority to enforce § 4 for any entities not subject to the jurisdiction of several listed federal financial regulators or state insurance authorities); Data Security and Breach Notification Act of 2015, H.R. 1770, 114th Cong. (2015) § 2 (requiring covered entities to implement and maintain reasonable security measures and practices to protect and secure electronic personal information) and § 4(a) (providing that a violation of § 2 would constitute an unfair and deceptive act or practice in violation of the FTC Act); Data Breach Notification and Punishing Cyber Criminals Act of 2015, S. 1027, 114th Cong. (2015) § 2 (generally requiring covered entities to take reasonable measures to protect and secure electronic data containing personal information) and § 4(c) (providing that a violation of § 2 shall be treated as an unfair or deceptive act or practice in violation of the FTC Act).

143 S. 961 and H.R. 2205 §4(a)(4)(D)(iii).

intrusions into, systems; incident response programs; and measures to protect against the destruction, loss, or damage of sensitive information due to environmental or technological failures;[144]

» requirements for board of director oversight, including having the board approve the company's written information security program; requiring the board to oversee the development, implementation, and maintenance of the program, including assigning specific responsibility for its implementation and reviewing reports from management; and requiring management to report to the board or a committee at least annually on the information security program and material matters relating to the program;[145] and

» breach investigation and notification requirements.[146]

These additional requirements would go a long way to minimizing the differences between the regulatory requirements applicable to banks and those applicable to non-banks, while still providing the flexibility necessary for companies of various sizes and levels of sophistication to enter and compete in the marketplace.

These bills would ensure that data security requirements are established by legislation, rather than through further rulemaking by the FTC (or any other agency) before they can be implemented.[147]

In order to exercise any new authority successfully, the FTC would also need to be provided with more resources to properly staff investigations and enforcement actions against APPs for potential violations of any new regulatory requirements. And, to avoid adding unnecessary, overlapping, and/or inconsistent regulations to entities (including banks) that are already heavily regulated in this area, any new authorities provided to the FTC should make clear that they are not applicable to firms subject to data security regulation by the prudential regulators.

As to the second category above, legislation might make clear that APPs are subject to the same type of scrutiny with respect to data security as banks, such as by directly giving the FTC or CFPB examination authority (without requiring further regulations to do so), or by directly requiring the CFPB to enact rules defining large participants in the APP industry. ■

144 Id. §4(a)(5)(A).

145 Id. §4(a)(6).

146 Id. §4(b) and (c).

147 While these bills are a significant first step, more may be needed in the future to ensure consistency in regulatory treatment, particularly with respect to those APPs that may already be subject to the FTC Safeguards Rule, where compliance with those data security regulations may be considered compliance with the data security standards included in those bills. For example, both S. 961 and H.R. 2205 would provide that financial institutions that maintain policies and procedures consistent with those policies and procedures designed to comply with the GLBA that are applicable to the financial institution would be deemed to be in compliance with the bills' data security requirements. Arguably, this could include financial institutions complying with the FTC Safeguards Rule. To effectively ensure that APPs are subject to any additional data security requirements in the Act beyond the FTC Safeguards Rule, the financial institutions exception may need to be limited to financial institutions subject to and in compliance with the Interagency Guidance, rather than all "financial institutions" broadly subject to and in compliance with even the more narrow FTC Safeguards Rule.