The Clearing House

August 2, 2019

Submitted electronically through https://www.regulations.gov/docket?D=FTC-2019-0019

David Lincicum and Allison M. Lefrak
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W., Suite CC-5610 (Annex B)
Washington, DC 20580

Re: Safeguards Rule, 16 CFR part 314, Project No. P14507

Dear Mr. Lincicum and Ms. Lefrak:

The Clearing House Association L.L.C ("The Clearing House")[1] appreciates the opportunity to comment on the Federal Trade Commission's ("FTC") April 4, 2019 Notice of Proposed Rulemaking and Request for Public Comment entitled "Standards for Safeguarding Customer Information,"[2] regarding the FTC's Gramm-Leach-Bliley Act ("GLBA") Safeguards Rule, codified at 16 C.F.R. part 314 (the "Safeguards Rule" or "Rule").

The Clearing House commends the FTC for proposing to provide more specific requirements for FTC-regulated institutions, including for their information security programs. These entities, including financial technology ("Fintech") companies, often engage in activities that are similar to many activities undertaken by banks subject to oversight by the federal prudential regulators. Financial institutions subject to the FTC's Safeguards Rule jurisdiction often collect and maintain many or all of the same data elements maintained by other financial institutions.

As explained further below and in our November 2016 letter in response to the FTC's 2016 request for public comment[3] (attached), since the adoption of the Safeguards Rule, the Fintech industry has grown

---

1 The Clearing House Association L.L.C is a nonpartisan organization that engages in research, analysis, advocacy and litigation focused on financial regulation that supports a safe, sound and competitive banking system.

2 Standards for Safeguarding Customer Information, 84 Fed. Reg. 13,158 (proposed Apr. 4, 2019) (to be codified at 16 C.F.R. pt. 314) (the "NPRM" or "Proposed Rule").

3 Standards for Safeguarding Customer Information, 81 Fed. Reg. 61,632 (Sept. 7, 2016).

rapidly, in parallel with, and on the foundation of, innovations in the technology and financial sectors. This has included an expansion, especially by alternative payment providers ("APPs") and data aggregators, into services traditionally offered exclusively by banks.[4] These companies hold vast amounts of consumer financial data. Proper handling of that information is essential both to the security of the information and to the safety and soundness of the financial system. As such, enhancing the security requirements that apply to these entities is critical to ensuring that consumers' financial information is protected regardless of the type of financial institution that maintains that information.

While the FTC's proposed revisions to the Safeguards Rule represent a substantial improvement over the status quo, The Clearing House remains concerned about the important differences that remain between the standards to which traditional financial institutions regulated by the prudential regulators are subject and those that the FTC has proposed in the NPRM. This is particularly concerning when institutions are subject to the FTC's jurisdiction, on the one hand, and those that are subject to the prudential regulators' jurisdiction, on the other, are engaged in functionally equivalent activities and often hold identical kinds of information.

In order to protect the confidentiality, integrity, and availability of consumer information on Fintech platforms, as well as the safety and soundness of the financial system, The Clearing House recommends that the FTC further strengthen the Safeguards Rule, beyond the enhancements proposed in the NPRM. At least with respect to large Fintech companies, these requirements should be more akin to the rules applicable to banks under the Federal Financial Institutions Examination Council ("FFIEC") Interagency Guidelines Establishing Information Security Standards ("Interagency Guidelines").

EXECUTIVE SUMMARY

In this letter, The Clearing House seeks to provide general feedback on the Proposed Rule. Our response also provides feedback on some of the particular questions posed by the NPRM, including "whether the use of the number of customers concerning whom the financial institution retains customer information is the most effective way to determine which financial institutions should be exempted,"[5] and "whether adding a breach notification requirement to the Rule would benefit consumers."[6]

---

4 For more information about APPs and data aggregators and their particular functionality, please see our November 2016 comment letter at 4-9.

5 NPRM, 84 Fed. Reg. at 13,171.

6 *Id.* at 13,170 n.123.

As described in our November 2016 comment letter, much has changed since the Safeguards Rule was promulgated in 2002. Those changes have only continued in the last few years. As a result of the growth of the Fintech industry, many Fintech companies hold substantial and constantly-increasing volumes of highly sensitive consumer financial information. While the proposed revisions to the Safeguards Rule would make enhancements to the security requirements that apply to these companies, the Proposed Rule is still lacking in comparison to the requirements that apply to banks. The changes in technology and economic conditions that have led to the explosive and continued growth of the Fintech sector continue to warrant the adoption of stricter, more robust data security requirements under the FTC Safeguards Rule, at least for Fintech companies.

As described in further detail below:

- Since 2016, the Fintech sector has continued to grow and expand into services traditionally provided by banks; however, appropriate security continues to lag. Studies show that overall investment in Fintech continues to grow rapidly, as does the number of consumers using these services. This investment and growth has not, however, been met by appropriate investment in security for these entities. The consumer risks from lax security in Fintech are exacerbated by the fact that many of the terms and conditions in Fintech offerings absolve the company of liability in the event of fraud. While Congress, regulators, and self-regulatory organizations have worked to improve standards and guidance applicable to certain industries and across the economy, the Safeguards Rule remains the primary regulatory standard applicable to Fintech companies.

- Despite the risks, while the Proposed Rule would make a number of improvements, gaps between the regulatory data security requirements in the Proposed Rule and the data security standards that apply to banks would remain. While both banks and many Fintech companies are subject to the GLBA data security requirements, banks are subject to detailed regulations and guidance documents promulgated by the financial regulatory agencies that make up the FFIEC, whereas Fintech companies are subject only to the FTC's Safeguards Rule. While the Proposed Rule has closed some of the key gaps we identified in our 2016 letter between these two regimes, key differences remain, including the level of detail, and the standards regarding board and management involvement, employee background checks, authentication, and data breach notification. The lighter substantive regulatory requirements, combined with limited liability pursuant to the terms and conditions described above, as well as the exceedingly low risk of enforcement action or monetary penalty resulting from noncompliance, would still result in materially weaker data security protections for consumers' financial information held by Fintech companies under the Proposed Rule as compared to the protections in place for banks when both are engaged in the same activities.

- The Clearing House recommends that the FTC enhance the Safeguards Rule by looking to the FFIEC requirements and guidance as models. The FFIEC Interagency Guidelines and IT Examination Handbook have been implemented by financial institutions and vendors across the country for several years and are comprehensive in their coverage. They therefore represent more appropriate models for the FTC to leverage in revising the Safeguards Rule rather than looking to the newer, less comprehensive, and less widely adopted New York Department of Financial Services ("NYDFS") Cybersecurity Requirements for Financial Services Companies or National Association of Insurance Commissioners ("NAIC") Insurance Data Security Model Law.

I. Since the FTC's 2016 Request for Comment, the Fintech Sector Has Continued to Grow and Expand into Traditional Bank Services.

In recent years, the Fintech industry has continued to evolve, in parallel with, and on the foundation of, innovations in the technology and financial sectors. This has included a continued expansion of the services offered by Fintech companies into many traditional banking services, especially by APPs, including peer-to-peer ("P2P") payment services, and data aggregators. Aggregators often gain direct access to consumers' financial accounts (including through the collection, storage, and use of financial account credentials).[7]

Rapid growth in this industry continues. According to Forbes, "overall investment in [F]intech surged in 2018, hitting $55 billion worldwide, double the year before."[8] Other estimates suggest the number could be substantially higher; for example, KPMG's biannual Fintech study found that total global investment dollars across mergers and acquisitions, private equity, and venture capital more than doubled year-over-year in 2018 to $111.8 billion, with $52.5 billion in investments in the U.S. alone (primarily through M&A).[9]

---

[7] Financial account credentials include bank-issued consumer account passwords and account IDs, as well as the consumer's pre-arranged responses to the banks' security questions. This information, if compromised, could be used by criminals in an attempt to defeat banks' authentication protocols.

[8] Jeff Kauflin et al., *The Most Innovative Fintech Companies in 2019*, Forbes (Feb. 4, 2019), https://www.forbes.com/fintech/2019/#328bea7a2b4c.

[9] KPMG, *The Pulse of Fintech 2018: Biannual Global Analysis of Investment in Fintech* at 2-3 (Feb. 13, 2019), https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/the-pulse-of-fintech-2018.pdf.

Nineteen of Forbes' "2019 Fintech 50" were valued at *$1 billion or more*.[10] A number of the additions to this year's Forbes list included payments technology companies.[11] Among the Fintech 50 are companies that use data aggregation, including:

- Acorns, an application-based investment vehicle. Acorns links to users' credit cards and checking accounts, then "rounds up" credit card transactions, withdraws the additional funds from the users' checking accounts, and invests the money in user-selected investment portfolios. While Acorns vaguely boasts on the sign-up page that it is "Protected with Bank Level Security,"[12] its staff of nearly 250 people boasts just a single employee (an "Information Security Engineer") with a clear security responsibility.[13]

- Even, a budgeting and savings application that links to users' bank accounts, collects information about upcoming bills, and estimates remaining funds to spend. Even assures customers that it can be trusted with their bank information by citing their Better Business Bureau rating and noting that it employs end-to-end encryption for users' connections with Even and that "Even's systems have been audited for security and compliance and regularly undergo security and privacy audits by some of the nation's largest employers."[14]

- Plaid, which connects APPs, such as Venmo and personal finance sites, "to users' bank accounts to transfer and track funds and speed up authentication."[15] For example, its "Auth" product "pulls users' account and routing information instantly," and its "Identity" product "confirms users' identities with what's on file at the bank—in other

---

10 Jeff Kauflin et al., *The Most Innovative Fintech Companies in 2019*, Forbes (Feb. 4, 2019), https://www.forbes.com/fintech/2019/#328bea7a2b4c.

11 *Id.*

12 Acorns, Create Account, https://signup.acorns.com/ (last visited July 29, 2019).

13 Acorns, About, Our Team, https://www.acorns.com/about/team/ (last visited July 29, 2019).

14 Even, FAQs, Connecting Your Bank and Security & Privacy, https://even.com/faq (last visited July 29, 2019).

15 *FinTech 50, Plaid*, Forbes (Feb. 4, 2019), https://www.forbes.com/companies/plaid/?list=fintech/#6fe827cc60d0 (last visited July 29, 2019).

The Clearing House

words, their name, phone number, address, and email."[16] Plaid's entire business model is to provide the data that other companies—like the companies described above and in The Clearing House's November 2016 letter—are using; its growth and valuation are driven by the number of customers to whom it is providing data. Plaid claims on its website that "tens of millions of people in North America (and counting) have successfully connected their accounts to apps they love using Plaid," and that it has analyzed over ten *billion* transactions.[17] And, due to recent developments in its Auth product, Plaid's application programming interface ("API") can now connect to *all* 11,500 U.S. banks and credit unions, irrespective of the technology used by any particular financial institution.[18] According to Forbes, Plaid is valued at $2.65 billion, and "[o]ne in four Americans with a bank account now uses Plaid (probably without realizing it)."[19]

Statista market analysis determined that digital payments is the largest Fintech market segment, with an expected total transaction value of over $4 *trillion* in 2019 worldwide,[20] and nearly $1 trillion in the United States alone.[21] Annual growth for the next 4 years is expected to be 8.6% in the United States and 12.8% worldwide, for an annual worldwide transaction value of nearly $6.7 trillion in 2023.[22]

---

16 Plaid, Use Cases: Banking and Brokerage, https://plaid.com/use-cases/banking-and-brokerage/ (last visited July 29, 2019).

17 Plaid, Inc., https://plaid.com/ (last visited July 29, 2019); Plaid, About Us: Company, https://plaid.com/company/ (last visited July 29, 2019).

18 *See* Ron Miller, *Plaid Expands Financial Service API to Include All US Banks*, TechCrunch (Feb. 5, 2019), https://techcrunch.com/2019/02/05/plaid-expands-finance-api-to-include-all-us-banks/.

19 *FinTech 50, Plaid*, Forbes (Feb. 4, 2019), https://www.forbes.com/companies/plaid/?list=fintech/#6fe827cc60d0.

20 Market Directory: FinTech Worldwide, Statista, https://www.statista.com/outlook/295/100/fintech/worldwide (last visited July 29, 2019).

21 Market Directory: FinTech United States, Statista, https://www.statista.com/outlook/295/109/fintech/united-states (last visited July 29, 2019).

22 Market Directory: Digital Payments United States, Statista, https://www.statista.com/outlook/296/109/digital-payments/united-states (last visited July 29, 2019); Market Directory: Digital Payments Worldwide, Statista, https://www.statista.com/outlook/296/100/digital-payments/worldwide (last visited July 29, 2019).

The Clearing House

Personal finance and "alternative lending" have consistently been the second and third biggest market segments in recent years, per Statista, with total transaction value for personal finance nearly doubling year-over-year worldwide in 2019 to over $1 trillion dollars, and alternative lending reaching almost $250 billion worldwide in 2019 (and over $750 billion and nearly $8.5 billion, respectively, in the United States).[23] In 2019, Statista estimates that over 270 million Americans use digital payments and nearly 50 million people worldwide (including 10 million Americans) use Fintech personal finance offerings.[24] According to TransUnion, Fintech companies issued 38% of all U.S. personal loans in 2018, up only marginally year-over-year, but up from a mere 5% in 2013.[25]

Despite the rapid growth and significant dollars being invested in the growing Fintech market, real security vulnerabilities remain. For example, according to a recent study sponsored by the Center for Financial Inclusion, "the integrity of data gathered from mobile money applications varied dramatically across the sample," and "neither presence in a developed market nor company maturity predicted

---

[23] Market Directory: Personal Finance Worldwide, Statista, https://www.statista.com/outlook/298/100/personal-finance/worldwide (last visited July 29, 2019); Market Directory: Alternative Lending Worldwide, Statista, https://www.statista.com/outlook/399/100/alternative-lending/worldwide (last visited July 29, 2019); Market Directory: Personal Finance United States, Statista, https://www.statista.com/outlook/298/109/personal-finance/united-states (last visited July 29, 2019); Market Directory: Alternative Lending United States, Statista, https://www.statista.com/outlook/399/109/alternative-lending/united-states (last visited July 29, 2019).

[24] Market Directory: Digital Payments United States, Statista, https://www.statista.com/outlook/296/109/digital-payments/united-states (last visited July 29, 2019); Market Directory: Personal Finance Worldwide, Statista, https://www.statista.com/outlook/298/100/personal-finance/worldwide (last visited July 28, 2019); Market Directory: Personal Finance United States, Statista, https://www.statista.com/outlook/298/109/personal-finance/united-states (last visited July 29, 2019). Statista defines the "digital payments" market as payments for products and services made online and mobile payments at point-of sale via smartphone applications, and defines "personal finance" market as automated investment services and cross-border fund transfers between private users. Market Directory: Digital Payments Worldwide, Statista, https://www.statista.com/outlook/296/100/digital-payments/worldwide (last visited July 29, 2019); Market Directory: Personal Finance Worldwide, Statista, https://www.statista.com/outlook/298/100/personal-finance/worldwide (last visited July 29, 2019).

[25] Kate Rooney, *Fintechs Help Boost US Personal Loan Surge to a Record $138 Billion*, CNBC (Feb. 24, 2019), https://www.cnbc.com/2019/02/21/personal-loans-surge-to-a-record-138-billion-in-us-as-fintechs-lead-new-lending-charge.html.

better security performance: similar security vulnerabilities were found in both early stage startups and more established providers and in institutions from all world regions in the sample."[26]

According to the study of 52 digital finance companies, including 14 in the U.S., 17 of the 27 studied companies with mobile applications use "demonstrably bad ciphering options" on their applications, while 11 companies' websites received a failing grade from Qualys Secure Socket Layer test's assessment of server configuration.[27] Overall, the research "found numerous egregious security errors in over half of the app[lications] . . . examined, including misuse of cryptography, use of weak cryptography, and excessive permission requirements,"[28] despite these issues being well known in the industry for years, thereby putting "both consumers and providers at severe risk of compromise."[29]

The Center for Financial Inclusion study also noted, as The Clearing House did in its November 2016 comment letter, that Fintech security risks are compounded by the fact that many of the terms and conditions in Fintech offerings absolve the company of liability in the event of fraud. This is possible because many of these companies are not subject to bank regulations that otherwise protect consumers from losses arising out of fraudulent uses of their accounts. The Center for Financial Inclusion study found that, where terms of service mentioned fraud being perpetrated against a user at all (8 out of the 33 companies with publicly-available terms of service), it did so only to exclude the Fintech company's liability as a condition of use of the service.[30] Particularly as Fintech growth has resulted in expanded use of their products by underserved communities—who are among the most vulnerable if their information is hacked—the combination of rapid growth, lax data security practices, and disclaimers on liability can be particularly dangerous for consumers.[31]

---

26 Pablo Anton-Diaz, *New Data Security Study of Fintech Apps Highlights Vulnerabilities*, Center for Financial Inclusion (Sept. 5, 2018), https://www.centerforfinancialinclusion.org/new-data-security-study-of-fintech-apps-highlights-vulnerabilities/.

27 Patrick Traynor, *Digital Finance and Data Security: How Private and Secure is Data Used in Digital Finance?*, Center for Financial Inclusion, at 3, 18, 24 (Sept. 2018), https://content.centerforfinancialinclusion.org/wp-content/uploads/sites/2/2018/09/CFI43-CFI_Online_Security-Final-2018.09.12.pdf.

28 *Id.* at 25. In this context, "permissions" refers to the types of approvals to access device data users are required to grant the application before being permitted to use the application—e.g., access to device ID, location, stored files, and call information.

29 *Id.*

30 *Id.* at 26-27.

31 *See, e.g.*, Claudi Ng, *Regulating Fintech: Addressing Challenges in Cybersecurity and Data Privacy*,

These concerns are only further heightened as technology companies that have not traditionally offered financial services have recently proposed to move into the financial sector through cryptocurrency and other offerings.[32]

Congress, regulators, and self-regulatory authorities continue to take an increased interest in these issues. For example, in 2018, FINRA published an investor alert, urging investors to exercise caution before ceding to the convenience of data aggregation.[33] In its alert, FINRA highlighted the security risks posed by many data aggregators, including "vulnerability to cyber fraud, unauthorized transactions and identity theft," arising in part from the fact that "aggregators could be storing *all* consumer financial information or security credentials in one place, creating a new and heightened security risk for consumers."[34] FINRA also highlighted the limited data security regulatory oversight and regulatory requirements, particularly as compared to registered financial institutions.[35]

Congress also continues to express a keen interest in enacting comprehensive data security legislation and/or legislating in sector-specific areas. According to the Congressional Research Service, between the 115th Congress and the first four months of the 116th Congress, nearly 40 cybersecurity bills have received some sort of committee action, received a vote and/or were passed by one chamber, or have been enacted into law.[36] Through May 1, 2019, there have been 20 hearings on cybersecurity-related issues this year alone, following the approximately 90 cybersecurity hearings held during the 115th

---

Harvard Kennedy School Government Innovators Network (Feb. 22, 2018), https://www.innovations.harvard.edu/blog/regulating-fintech-addressing-challenges-cybersecurity-and-data-privacy.

32 *See, e.g.*, Nichols Megaw, *BIS Warns on Facebook Risk to Finance After Libra Plan Unveiled*, Financial Times (June 23, 2019), https://www.ft.com/content/db37a29e-95a8-11e9-8cfb-30c211dcd229 ("Big tech groups such as Facebook could 'rapidly establish a dominant position' in global finance and pose a potential threat to competition, financial stability and social welfare, according to the Bank for International Settlements," the "central bank for central banks.").

33 FINRA, Know Before You Share: Be Mindful of Data Aggregation Risks (Mar. 29, 2018), http://www.finra.org/investors/alerts/know-you-share-be-mindful-data-aggregation-risks.

34 *Id.*

35 *Id.*

36 Rita Tehan, Cong. Research Serv., R43317, Cybersecurity: Legislation & Hearings: 115th-116th Congress (Updated May 2, 2019), https://www.everycrsreport.com/files/20190502_R43317_86546263c4d557161e8c9f031b9bdc2ccc016ff5.html.

Congress.[37] Among these hearings were House Financial Services Committee hearings on legislative proposals to reform data security and breach notification regulatory regimes and on data security vulnerabilities and opportunities for improvement, as well as a Senate Banking Committee hearing on cybersecurity risks to the financial services industry.[38]

The FTC has also recently held sessions on data security, including a two-day data security hearing in December 2018, as part of the FTC's extensive competition and consumer protecting hearing series.[39] And in May 2019, the FTC announced a new dedicated FTC Business Center page for Fintech companies, including links to a number of cybersecurity guidance documents and resources,[40] underscoring the FTC's appreciation of the unique significance of Fintech cybersecurity.

II. While the Proposed Changes to the Safeguards Rule Represent Substantial Improvement, Important Gaps Between the Safeguards Rule and FFIEC Requirements Remain.

While both banks and many Fintech companies are subject to the data security requirements established in the GLBA, even under the Safeguards Rule as proposed in the NPRM, the two groups would continue to operate under quite different sets of implementing regulations and regulatory guidance. Banks are subject to the more detailed and demanding standards adopted jointly by the federal financial regulatory agencies, while those Fintech companies covered by the GLBA are subject to the more general Safeguards Rule promulgated by the FTC, which would remain less detailed under the Proposed Rule. The resulting lighter substantive requirements, combined with decreased odds of

---

37 *Id.*

38 *Id.* (*Legislative Proposals to Reform the Current Data Security & Breach Notification Regulatory Regime: Hearing Before the H. Comm. on Fin. Servs.*, 115th Cong. (2018); *Cybersecurity: Risks to the Financial Services Industry & Its Preparedness: Hearing Before the S. Comm. on Banking, Housing, & Urban Affairs*, 115th Cong. (2018); *Data Security: Vulnerabilities & Opportunities for Improvement: Hearing Before the H. Comm. on Fin. Servs.*, 115th Cong. (2017)).

39 FTC, Hearings on Competition & Consumer Protection in the 21st Century, Hearing #9: Data Security (Dec. 11-12, 2018), https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-december-2018.

40 FTC, Business Center: FinTech, https://www.ftc.gov/tips-advice/business-center/credit-and-finance/fintech; Press Release, FTC, *FinTech Finds a Home in the FTC Business Center* (May 24, 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/05/fintech-finds-home-ftc-business-center.

enforcement actions and less prospect of substantial monetary sanctions for violations,[41] mean weaker data security protections for consumers' financial information when it is held by Fintech companies.

A. Prudential Regulators and the Interagency Guidelines.

---

[41] Since the effective date of the FTC Safeguards Rule 16 years ago, the FTC has brought almost 30 cases involving GLBA violations. *See* FTC, Privacy & Data Security Update: 2018, at 6, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf. Only approximately half of those, however, have alleged violations of the GLBA Safeguards Rule. In the years since The Clearing House's November 2016 comment letter, the FTC has brought only two enforcement actions alleging violations of the Safeguards Rule: *TaxSlayer, LLC*, FTC Matter/File No. 162 3063; and *PayPal, Inc.*, FTC Matter/File No. 162 3102. GLBA Safeguards Rule enforcement actions often result in consent orders providing only for non-monetary sanctions (e.g., a requirement to comply with the Rule, that is, doing what the respondent company should have been doing already), unless the FTC also alleges violations of statutes that grant the FTC separate authority to levy penalties (e.g., the Fair Credit Reporting Act ("FCRA")). *See, e.g.*, Stipulated Final Judgment & Order for Payment of Civil Penalties, *United States v. PLS Financial Servs., Inc.*, Case No. 1:12-cv-8334 (N.D. Ill. 2012) (settlement imposing $101,500 civil penalty for FCRA violations as well as non-monetary sanctions for alleged violations of the FTC Act, FCRA, the Disposal Rule, and the GLBA Safeguards and Privacy Rules).

The provision that grants the FTC and the prudential regulators GLBA enforcement authority provides that they shall enforce the GLBA in accordance with their respective organic statutes—in the case of the FTC, the FTC Act. *See* 15 U.S.C. § 6805(a). We understand that, while the FTC has broad authority to bring suits to enforce the FTC Act, the FTC is not authorized to assess civil penalties for initial violations of the Safeguards Rule. *Compare* 15 U.S.C. § 57b(a)(1), (b) *with* 15 U.S.C. § 1681s. *See* U.S. Gov't Accountability Office, GAO-19-196, Consumer Data Protection: Actions Needed to Strengthen Oversight of Consumer Reporting Agencies 18 (2019) ("FTC's civil penalty authority does not extend to initial violations of GLBA's . . . safeguarding provisions . . . . For violations of GLBA provisions, which are enforced pursuant to FTC Act authority, FTC may seek an injunction to stop a company from violating these provisions and may seek redress (damages to compensate consumers for losses) or disgorgement."). Because determining the consumers affected and the amount of harm suffered can be difficult, FTC staff have asserted that it is difficult for the agency to obtain related redress. *See id.* at 18-19 ("[D]etermining the appropriate amount of consumer compensation requires FTC to identify the consumers affected and the amount of monetary harm they suffered. In cases involving security or privacy violations resulting from data breaches, assessing monetary harm can be difficult. Consumers may not be aware that their identities have been stolen as a result of a breach and or identity theft, and related harm may occur years in the future. In addition, it can be difficult to trace instances of identity theft to specific data breaches. According to FTC staff, these factors can make it difficult for the agency to identify which individuals were victimized as a result of a particular breach and to what extent they were harmed and then obtain related redress or disgorgement."). Because (1) FTC enforcement actions involving the Safeguards Rule are rare and (2) the likelihood of monetary penalties being assessed in such cases is even more rare, there is currently insufficient deterrent to encourage compliance.

Bank GLBA data security requirements have been laid out in the prudential regulators' Interagency Guidelines.[42] Under the Interagency Guidelines, financial institutions' information security programs must include six components: (i) board of directors' involvement, including at least annual reporting to the board; (ii) risk assessment; (iii) risk management and control; (iv) oversight of service providers; (v) an incident response program; and (vi) periodic updating. The Interagency Guidelines provide detailed requirements for each of these six components.

The Interagency Guidelines have been supplemented by various guidance documents issued by the FFIEC member agencies. These include the FFIEC's IT Examination Handbook, especially its Information Security, Outsourcing Technology Services, and Supervision of Technology Service Providers booklets[43] as well as topical bulletins that include information security components,[44] and other guidance documents, such as the Cybersecurity Assessment Tool.[45] The IT Examination Handbook's Information Security booklet alone contains nearly 90 pages of detailed security guidance, including information on implementation of specific security controls (ranging from remote access to encryption key management) and security monitoring.[46]

---

42 12 C.F.R. pt. 30, app. B (as incorporated into the OCC regulations for national banks). In addition 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, broker-dealers, investment companies, and investment advisers.

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

44 *See, e.g.*, FFIEC, Joint Statement on Cybersecurity of Interbank Messaging and Wholesale Payment Networks, http://www.ffiec.gov/press/PDF/Cybersecurity_of_IMWPN.pdf; FFIEC, Joint Statement on Cyber Attacks Involving Extortion, https://www.ffiec.gov/press/PDF/FFIEC%20Joint%20Statement%20Cyber%20Attacks%20Involving%20Extortion.pdf; OCC Bulletin 2013-29, Third-Party Relationships, Risk Management Guidance (Oct. 30, 2013), 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 (June 28, 2011), https://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf; FFIEC, Joint Statement on Cyber Insurance and Its Potential Role in Risk Management Programs, https://www.ffiec.gov/press/pdf/FFIEC%20Joint%20Statement%20Cyber%20Insurance%20FINAL.pdf.

45 FFIEC, Cybersecurity Assessment Tool (Aug. 29, 2018), https://www.ffiec.gov/cyberassessmenttool.htm.

46 FFIEC IT Examination Handbook, Information Security Booklet (Sept. 2016), http://www.ffiec.gov/press/PDF/FFIEC_IT_Handbook_Information_Security_Booklet.pdf.

B. The Commission's Safeguards Rule.

While most Fintech companies are likely subject to the GLBA's data security requirements,[47] they do not have to follow the Interagency Guidelines. Instead, they are subject to the FTC's Safeguards Rule.[48] 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 differences between the data security requirements imposed on banks by the Interagency Guidelines and those currently applicable to Fintech (and other) companies under the Safeguards Rule as it currently stands are numerous, even though the information held by banks and Fintech companies and risks attendant to each may be identical.

In our November 2016 comment letter, we highlighted six fundamental differences between the Safeguards Rule and Interagency Guidelines. The proposed amendments to the Safeguards Rule address some of these distinctions. Most notably, we commend the FTC's proposal to enhance the service provider oversight requirements in the Safeguards rule. While the current Safeguards Rule requires FTC-regulated financial institutions to oversee service providers in the selection, retention, and contracting phase,[49] the Interagency Guidelines and other guidance issued by the prudential regulators require banks to go beyond this initial oversight by taking an active role in overseeing the data security practices of their service providers on an ongoing basis. For example, in addition to conducting due diligence in selecting service providers and including data security requirements in service provider contracts[50], the Interagency Guidelines require banks, where indicated by their risk assessments, 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."[51] This requirement is

---

47 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" and "[p]roviding financial . . . or economic advisory services"). 12 U.S.C. § 1843(k)(4)(A), (C).

48 16 C.F.R. pt. 314.

49 16 C.F.R. § 314.4(d).

50 12 C.F.R. pt. 30, app. B, § III(D)(1-2).

51 *See* 12 C.F.R. pt. 30, app. B, § III(D)(3).

supplemented by the FFIEC IT Examination Handbooks' Outsourcing Technology Services booklet, which includes an entire section on ongoing monitoring of service providers.[52]

Under the Safeguards Rule, by contrast, Fintech companies are currently free from any express regulatory requirement mandating such ongoing vendor supervision. The proposed changes outlined in the NPRM would address this gap by adding requirements that financial institutions periodically assess service providers "based on the risk they present and the continued adequacy of their safeguards."[53] Third-party service providers continue to be a significant vector for data breaches, presenting a risk that cannot be fully mitigated at the onboarding stage.[54] The Clearing House welcomes this important change in the Proposed Rule, which is critical to protecting consumers.

Despite this (and other) important enhancements included in the NPRM, other key distinctions between the Safeguards Rule and Interagency Guidelines/FFIEC guidance that we identified in our November 2016 letter remain even in the Proposed Rule.

First, while the proposed revisions to the Safeguards Rule substantially increase the level of detail in its requirements, there remains a significant difference in level of detail between the two regimes. This has real implications for types of data security precautions regulators can reasonably demand, and consumers should reasonably expect, from banks, on the one hand, and non-bank Fintech companies, on the other. For example, unlike the requirements applicable to banks, the amended Safeguards Rule as proposed in the NPRM would have no express requirements for (1) business continuity programs, (2) network segmentation, (3) anti-malware or anti-virus protection, or (4) dual control procedures. By contrast, no reasonable bank could argue that it is not expected to maintain a business continuity program to plan for contingencies due to potential environmental or technological failures,[55] implement network segmentation and other network-based controls,[56] deploy tools to identify and protect against

---

52 FFIEC IT Examination Handbook, Outsourcing Technology Services Booklet (June 2004), https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx.

53 16 C.F.R. § 314.4(f)(3) (as proposed to be revised).

54 *See, e.g.*, Press Release, Opus, *Opus & Ponemon Institute Announce Results of 2018 Third-Party Data Risk Study: 59% of Companies Experienced a Third-Party Data Breach, Yet Only 16% Say They Effectively Mitigate Third-Party Risk*s (Nov. 15, 2018), https://www.businesswire.com/news/home/20181115005665/en/Opus-Ponemon-Institute-Announce-Results-2018-Third-Party.

55 12 C.F.R. pt. 30, app. B, § III(C)(1)(h); FFIEC IT Examination Handbook, Information Security Booklet § II(C)(21).

56 FFIEC IT Examination Handbook, Information Security Booklet § II(C)(6), (9).

malware,[57] or implement dual-control procedures for employees with responsibilities for or access to customer information,[58] each of which is explicitly identified in the Interagency Guidelines and/or FFIEC IT Examination Handbook Information Security Booklet. While many of these gaps—as well as the gaps described below—are gaps between the Safeguards Rule and the Interagency Guidelines, these gaps are only compounded by the detailed supplemental guidance from the FFIEC in the form of individual guidance documents and the IT Examination Handbook. The lack of inclusion of some of these control requirements is particularly surprising in light of the FTC's clear view—reflected in its non-Safeguards Rule data security-related enforcement cases and other FTC guidance—that these are important components of a "reasonable" security program.[59]

Second, the Interagency Guidelines require involvement from bank leadership at the highest level, including boards of directors and senior management.[60] Under the Interagency Guidelines, 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.[61] While the revised FTC Safeguards Rule would, for the first time, require entities subject to the Safeguards Rule to involve their boards (or equivalent governing bodies) through annual reports,[62] the rules applicable to banks require board involvement not only in overseeing the *maintenance* of the information security program, but also in approving and overseeing the development and implementation of the program.[63] Furthermore, the FFIEC regulations and guidance require management involvement beyond the CISO,[64] whereas the FTC Safeguards Rule would

---

57 FFIEC IT Examination Handbook, Information Security Booklet § II(C)(12).

58 12 C.F.R. pt. 30, app. B, § III(C)(1)(e).

59 *See, e.g.*, FTC, Start with Security: A Guide for Business at 7-8 (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; FTC, Protecting Personal Information: A Guide for Business at 10 (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

60 12 C.F.R. pt. 30, app. B, § III(A), (F); FFIEC IT Examination Handbook, Information Security Booklet § I.

61 12 C.F.R. pt. 30, app. B, § III(A), (F).

62 16 C.F.R. § 314.4(i) (as proposed to be revised).

63 12 C.F.R. pt. 30, app. B, § III(A)(2).

64 *See, e.g.*, FFIEC IT Examination Handbook, Information Security Booklet § I.

apparently limit required management responsibility to the CISO.[65] The requirement for broad management responsibility for security is, at least in part, due to regulators' recognition that an effective information security program requires that security be "deeply embedded" in the institution's culture—where "management and employees are committed to integrating the program into the institution's lines of business, support functions, and third-party management program."[66] Particularly with rapidly growing start-up companies with small staffs but large volumes of consumer financial information, the continued lack of a requirement for ongoing management involvement beyond the CISO may well result in data security being given lower priority than growing the business's consumer base and ensuring a quick return on investment.

Third, recognizing the significant risk posed by insider threats, the Interagency Guidelines require banks to consider, and, if appropriate, adopt, employee background checks for employees with responsibilities for or access to customer information.[67] The IT Examination Handbook's 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.[68] These should be supplemented, according to the FFIEC, through the use of confidentiality and non-disclosure agreements.[69]

While the proposed revisions to the Safeguards Rule will enhance the employee training requirements compared to the current Rule,[70] the Rule would still lack a similar requirement with respect to employee background checks. This is compounded by the Proposed Rule's lack of a requirement for segregation of duties (which the Interagency Guidelines and FFIEC Information Security Booklet do include[71]), meaning employees with significant access to company systems and not subject to background check

---

65 16 C.F.R. § 314.4(a) (as proposed to be revised).

66 FFIEC IT Examination Handbook, Information Security Booklet § I(A).

67 12 C.F.R. pt. 30, app. B, § III(C)(1)(e).

68 FFIEC IT Examination Handbook, Information Security Booklet § II(C)(7)(a).

69 *Id.* § II(C)(7)(d).

70 *See* 16 C.F.R. § 314.4(e)(1)-(4) (as proposed to be revised).

71 12 C.F.R. pt. 30, app. B, § III(C)(1)(e); FFIEC IT Examination Handbook, Information Security Booklet § II(C)(7)(c).

requirements would have largely unfettered access to such systems. 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 may put customer data at risk.[72]

Fourth, guidance issued by the FFIEC agencies concerning 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.[73] The FTC Safeguards Rule, even as amended, imposes no similar specific requirement on Fintech companies. While the revised Rule would require FTC-regulated financial institutions to use multi-factor authentication for individuals accessing *internal* networks that contain customer information (i.e., for company employees),[74] it imposes no requirements for securing the consumer/user authentication process.

This is particularly problematic in light of many Fintech companies'—and particularly data aggregators—lax security practices around authentication. For example, while banks have worked with almost all such entities to provide consumer data via APIs, a number still collect data by first collecting the consumers' financial account log-in information (including usernames, passwords, and even sometimes security questions and answers) and then scraping the data.[75] Many also do not track "known" devices— i.e., devices historically associated with a secure user log-in session. While banks will

---

72 *See, e.g.*, Marc van Zadelhoff, *The Biggest Cybersecurity Threats Are Inside Your Company*, Harvard Bus. Rev. (Sept. 19, 2016), https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company.

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

74 16 C.F.R. § 314.4(c)(6) (as proposed to be revised).

75 As noted in The Clearing House's November 2016 comment letter, collection of data through bank-approved data feeds (e.g., via API) is most common when a bank commissions the aggregation services or when a bank contractually agrees to such access in exchange for access controls and limitations. In those cases, banks may impose contractual security requirements to protect consumer information and ensure bank compliance with its third-party oversight obligations under the Interagency Guidelines and FFIEC guidance documents. However, this effectively results in banks, not regulators, becoming the oversight authority in this space via enforcement of contractual violations. This risks putting banks in precarious situations where, for example, data aggregators are not willing to contract to a certain level of data security protections. In such cases, banks may be required not only to decline to contract with those entities, but to implement technological safeguards (to the extent possible) to preclude those entities from scraping. Ultimately, this could result in a barrier to consumer access to services that they want and could have if regulators stepped in to take on their appropriate enforcement role with data aggregators rather than relying on banks to do so.

generally use device history as a factor in determining when a user should be prompted to answer additional "challenge" questions before being permitted access to an account, some data aggregators pose challenge questions only at initial sign-up or at the account-linking stage, but not as banks tend to apply them—for any user session initiated from an "unknown" device. Because of these ongoing insecure practices, particularly when viewed in light of the history of Fintech security incidents involving authentication issues and the overall increase in credential-stuffing (also referred to as list validation or password spraying) attacks,[76] it is important that the FTC use this opportunity to impose increased authentication security requirements upon FTC-regulated financial institutions.

Finally, while the proposed Safeguards Rule amendments would, for the first time, mandate that FTC-regulated financial institutions (except those subject to the new "small business" exception[77]) create an incident response plan,[78] the Safeguards Rule still would not include an independent breach notification requirement akin to the one required for FFIEC-regulated financial institutions. Instead it would simply require that incident response plans document any notification or reporting requirements imposed by other state or federal laws.[79] This gap is particularly disappointing in light of the kinds of consumer financial information held by Fintech companies, particularly data aggregators' use of customer bank account log-in information, the breach of which could have serious implications for the safety and soundness of the financial system as a whole.

The FTC generally appears to be deferring to state data breach notice laws in its preliminary determination not to include a breach notice requirement.[80] While all 50 states, D.C., and a number of U.S. territories have enacted data breach notification laws, they remain a patchwork, covering different

---

76 *See, e.g.*, The Clearing House November 2016 comment letter at 9-12; Lily Hay Newman, *Hacker Lexicon: What is Credential Stuffing*, Wired (Feb. 17, 2019), https://www.wired.com/story/what-is-credential-stuffing/ (noting that credential stuffing attacks have been a problem for the last several years, but that there has been a recent rise in successful campaigns following recent hacker postings of voluminous, aggregated credential collections from multiple data breaches). *See also* Complaint at 4, *TaxSlayer, LLC*, FTC Matter/File No. 162 3063 (Oct. 20, 2017) (alleging that TaxSlayer failed to implement information safeguards to control the risks to customer information from inadequate authentication, including by failing "to implement adequate risk-based authentication measures sufficient to mitigate the risk of list validation attacks when such attacks became reasonably foreseeable.").

77 16 C.F.R. § 314.6 (as proposed to be revised).

78 *Id.* § 314.4(h) (as proposed to be revised).

79 *Id.* § 314.4(h)(6) (as proposed to be revised).

80 *See* NPRM, 84 Fed. Reg. at 13,170 n.123.

types of information and triggered in different circumstances. For example, while a growing number of states are amending their data breach notification laws to include usernames and passwords and/or security questions and answers in their definitions of personal information (either generally or when the credentials permit access to a financial account),[81] a substantial portion of states do not include this data element.[82] Therefore, without a specific breach notice requirement in the FTC Safeguards Rule, FTC-regulated financial institutions may be required to notify some consumers only in some states if a breach results in a compromise of consumer banking credentials.[83]

---

81 Cal. Civ. Code § 1798.82(h)(2) (defining "personal information" to include "[a] user name or email address, in combination with a password or security question and answer that would permit access to an online account"); D.C. Code § 28-3851(3)(A)(ii) (defining personal information to include "[a]ny other number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual's financial or credit account"); Pub. L. 2019, ch. 95 § 1 (New Jersey bill, signed into law by Governor Phil Murphy on May 10, 2019, amending N.J. Stat. § 56:8-161 to include "user name, email address, or any other account holder identifying information, in combination with any password or security question and answer that would permit access to an online account" in the definition of "personal information" under New Jersey's data breach notification law).

82 Conn. Gen Stat. § 36a-701b(a)(2) (defining "personal information" as name in combination with (1) Social Security Number; (2) driver's license number or state identification card number; (3) credit or debit card number; or (4) financial account number in combination with any required security code, access code, or password that would permit access to an individual's financial account); N.Y. Gen. Bus. Law § 899-aa(1)(b) (defining "private information," the breach of which is subject to data breach notification requirements, as an identifier in combination with (1) Social Security Number; (2) driver's license number or non-driver identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account).

83 In light of the limitations on the FTC's ability to enforce initial violations of the Safeguards Rule via civil penalties, *see* note 43, *supra*, The Clearing House appreciates the FTC's hesitation that such a requirement "would have limited effect." *See* NPRM, 84 Fed. Reg. at 13,170 n.123. However, just as this has not deterred the FTC from proposing any other new requirements in the NPRM, this should not deter the FTC from including a breach notification requirement. At minimum, the FTC would be able to enforce such a breach notice requirement in the same manner as it enforces the remaining requirements of the Safeguards Rule. Particularly in the context of breach notification, the FTC's ability to enforce violations of consent orders would be a useful tool to preclude FTC-regulated financial institutions from violating the requirement again.

Furthermore, the FTC continues to request that Congress provide it with civil penalty authority for GLBA violations. *See, e.g.*, *Hearing on Improving Data Security at Consumer Reporting Agencies Before the H. Comm. on Oversight & Reform, Subcomm. on Economic & Consumer Policy*, 115th Cong. (2019) (statement

III. The Interagency Guidelines, Not the NYDFS Cybersecurity Regulations or NAIC Model Law, Offer the Best Model for an Updated FTC Safeguards Rule.

Cybersecurity statutory mandates, regulatory frameworks, and administrative guidance are being tightened throughout the financial services sector in recognition of ever-increasing cybersecurity risks. Both Congress and regulators have recognized that the extent of regulatory requirements and guidance should be commensurate with the risks presented by covered entities' businesses. In assessing the risk profile for Fintech companies, it is important to remember that these companies do not just store personally identifiable information. They collect, process, and handle particularly sensitive financial account information in the ordinary course and have actively sought to be engaged in such business. It is precisely because of the heightened risks attached to unauthorized access to and disclosure of this sensitive financial account information, ranging from identity theft to account takeover, that lawmakers and regulators have imposed more stringent requirements upon banks through the GLBA and the Interagency Guidelines. Because of similar risks, banks and Fintech companies engaging in functionally similar activities and possessing comparable types and volumes of consumer data must be subject to similar, heightened regulatory regimes. The continued existence of gaps in the Safeguards Rule has significant implications for risks to consumers and to the safety and soundness of the financial system.

---

of the FTC 8), https://www.ftc.gov/system/files/documents/public_statements/1508935/p180101_ftc_testimony_re_oversight_house_12262019.pdf. Having a regulatory breach notice requirement in place would lay the groundwork for civil penalty authority over violations of such a requirement if Congress amends the FTC's enforcement authority, rather than requiring a subsequent additional rulemaking process.

We do appreciate, however, the FTC's concern about the potential that an FTC breach notice requirement would exempt financial institutions from breach notification laws with states that exempt companies in compliance with GLBA. *See* NPRM, 84 Fed. Reg. at 13,169-70. While a full 50-state survey of all such laws is beyond the scope of this letter, we generally assess that there is a relatively low likelihood that financial institutions that would otherwise be subject to penalties under a state breach notice law would be exempted from such penalties if the Safeguards Rule were amended to include a breach notice requirement, assuming an FTC breach notice requirement were drawn in line with the most common elements of the state notice statutes. *First*, many, if not all, of the states that include a GLBA exemption in their state notice statute word the exemption similarly to the Delaware statute cited in the Federal Register notice—namely, by exempting only those institutions that maintain procedures *pursuant to* the GLBA requirements and notify consumers *in accordance with* those procedures. NPRM, 84 Fed. Reg. at 13,169-70 (quoting Del. Code tit. 6, sec. 12B-103(b)). Thus, to the extent an FTC-regulated financial institution were to not comply with a theoretical FTC Safeguards Rule breach notice requirement, they would not be deemed in compliance with an otherwise-applicable state data breach notification statute (if the state statute were formulated in a similar manner to the Delaware statute). And second, as noted above, many state statutes do not require breach notification in the event of a credential breach alone—such that those breaches would not currently be subject to state notice requirements in any event.

We appreciate that, in revising the Safeguards Rule, the FTC is trying to take a less detailed approach that may be appropriate for "mom and pop shops" and other financial institutions engaging in lower risk businesses. And while we generally recognize the FTC's desire to exempt certain entities with a lower risk profile from certain requirements of the Proposed Rule, The Clearing House does not consider the manner in which the FTC has formulated the "small business" exemption to be appropriate. In particular, the exemption provides an arbitrary cutoff for companies based on the number of consumers (5,000) about whom a financial institution maintains information.[84] The Clearing House submits that the number of consumers about whom a financial institution maintains information is not the appropriate metric for determining size or a firm's capability to implement the requirements.

Instead, to the extent there is a bifurcation in the security requirements that apply to various types of FTC-regulated financial institutions, this should be based upon the sensitivity of an institution's activities and the data it maintains, rather than a bright-line rule based on the number of customers alone. For example, a bank with two branches in a rural county with a small customer base is still required to follow the data security requirements under the Interagency Guidelines, in recognition of the fact that consumers of small financial institutions should have the same protection for their sensitive financial information as do customers of large banks.

While the flexible, high-level approach that the FTC has proposed may be appropriate for financial institutions engaging in lower risk businesses, this approach continues to be inappropriate for Fintech companies, such as APPs and data aggregators, and the risks posed by their data collection and processing activities. A significantly more robust approach for Fintech companies is critical to ensuring that consumers enjoy consistent protection regardless of their choice of platform and to protect the safety and soundness of the financial system. In providing comprehensive and specific regulatory requirements for banks engaged in these activities, the regulators have recognized that certain higher-risk activities require a baseline set of controls that should be in place. Because of the similar risks posed to consumers and the safety and soundness of the financial system by a potential data security incident involving these types of Fintech companies, it is imperative that these companies be subject to regulatory requirements that provide far more specifics than the high-level approach taken under the current Safeguards Rule. Fintech companies continue to grow at rapid speed, including by expanding into underserved markets, aided by substantial investment. Often, these companies appear to offer consumers appealing convenience and innovation. However, these consumers are likely unaware of the different regulatory playing field and overall lower data protection standards applicable to these companies as compared to traditional financial institutions. It is therefore particularly critical for the FTC to ensure that the appropriate security framework is in place to protect consumers.

---

[84] 16 C.F.R. § 314.6 (as proposed to be revised).

While we appreciate the FTC's attempt to leverage some existing regulatory frameworks rather than creating yet another new additional cybersecurity standard, the Interagency Guidelines and FFIEC guidance collectively serve as a far more appropriate model than the NYDFS cybersecurity regulations or the NAIC Model Law. The regulations and guidance issued by the FFIEC have been in place for many years, are widely used throughout the financial sector (including by financial institutions' vendors and partners), are comprehensive, and appropriately risk tailored. By contrast, the NYDFS cybersecurity regulations are adopted in only one state (albeit one that affects many financial institutions) and the NAIC Model Law has been revised as it has been adopted. Both are only approximately two years old, and there is limited experience with their adoption to assess the extent to which they reflect an appropriately comprehensive security program.

Notably, the substantive scope of the FTC's statutory rulemaking authority under the GLBA is the same as that of the prudential regulators, who, as described above, have issued significantly more detailed and expansive data security regulations under the GLBA. In light of its equivalent authority, as well as the changes in the industry and the risks to consumers and the safety and soundness of the financial system, the FTC should use its authority to adopt enhanced GLBA Safeguards Rules based on the Interagency Guidelines.[85]

At minimum, these enhanced rules should include express regulatory requirements addressing the key outstanding gaps between the Interagency Guidelines and the Safeguards Rule identified above. These rules can either be limited to certain categories of Fintech companies (in which case the covered categories of institutions 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.

IV. Conclusion

We appreciate the work that the FTC is doing to enhance the Safeguard's Rule as well as this opportunity to comment on the proposed revisions. We hope that the FTC will take the points made above into consideration. In updating the Safeguards Rule, the FTC has an important opportunity to take action in an area of increased risk both to consumers and to the safety and soundness of the financial system. If you have any questions, please contact the undersigned by phone at (336) 769-5314 or by email at Rob.Hunter@theclearinghouse.org.

---

[85] One option would be for the FTC to issue Safeguards Rules that more closely align with the Interagency Guidelines, to be further supplemented by interpretive guidance similar to the FFIEC IT Examination Handbook and other guidance documents. In determining whether such an approach is appropriate, the FTC should consider the scope of its enforcement authority, which expressly excludes violations of interpretive rules. *See* 15 U.S.C. § 57b(a)(1).

Respectfully submitted,

/S/

Robert C. Hunter
Director of Legislative & Regulatory Affairs
& Deputy General Counsel
The Clearing House Association L.L.C.

Attachment

The Clearing House®
At the Center of Banking Since 1853®

November 21, 2016

Via Electronic Submission

David Lincicum and Katherine McCarron
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W., Suite CC-5610 (Annex B)
Washington, DC 20580

Re: Safeguards Rule, 16 CFR 314, Project No. P14507 (Standards for Safeguarding Customer Information; RIN 3084-AB35)

Dear Mr. Lincicum and Ms. McCarron:

The Clearing House Association L.L.C.[1] appreciates the opportunity to comment on the Federal Trade Commission's September 7, 2016 request for public comment entitled "Standards for Safeguarding Customer Information," regarding the regulations codified at 16 C.F.R. Part 314.[2]

As explained further below, the financial technology ("Fintech") industry has evolved rapidly in recent years, with many of these companies now offering to consumers payment and other services traditionally associated with banks. Many Fintech companies now handle large amounts of sensitive personal financial information, and yet they remain subject only to the high-level, general security standards in the FTC's Safeguards Rule.

FTC Commissioner Terrell McSweeny rightfully noted during her opening remarks at the FTC's recent Fintech series event on Crowdfunding and Peer-to-Peer payments that, in light of the recent growth of Fintech, it is important to ask how Fintech platforms ensure that fund

---

1 The Clearing House is a banking association and payments company that is owned by the largest commercial banks and dates back to 1853. The Clearing House Association L.L.C is a nonpartisan organization that engages in research, analysis, advocacy and litigation focused on financial regulation that supports a safe, sound and competitive banking system. Its affiliate, The Clearing House Payments Company L.L.C., owns and operates core payments system infrastructure in the United States and is currently working to modernize that infrastructure by building a new, ubiquitous, real-time payment system. The Payments Company is the only private-sector ACH and wire operator in the United States, clearing and settling nearly $2 trillion in U.S. dollar payments each day, representing half of all commercial ACH and wire volume.

2 Standards for Safeguarding Customer Information, 81 Fed. Reg. 61632 (Sept. 7, 2016) (hereinafter, the "Request").

transfers are appropriately directed; how consumers can obtain recourse in the event of a problem using these programs; how Fintech services protect the privacy and security of consumers' data; and how all of these protections compare to those implemented by prudentially-regulated financial institutions that have traditionally overseen funds transfers and payments.[3] In order to protect the confidentiality, integrity, and availability of consumer information on Fintech platforms, as well as the safety and soundness of the financial system, The Clearing House recommends that the FTC strengthen the Safeguards Rule with more detailed security requirements. At least with respect to large Fintech companies, these requirements should be more akin to the rules applicable to banks under the Federal Financial Institutions Examination Council ("FFIEC") Interagency Guidelines.

I. Executive Summary

In this letter, The Clearing House particularly seeks to respond to Question A.11 in the FTC's Request for Public Comment, which asks: "What modifications, if any, should be made to the Rule to account for changes in relevant technology or economic conditions?"

Much has changed since the Safeguards Rule was promulgated in 2002. As a result of the growth of the Fintech industry, many Fintech companies now hold substantial volumes of highly sensitive consumer financial information. These companies, however, are subject only to the very general requirements of the Safeguards Rule, and not the stricter data security requirements applicable to banks. The changes in technology and economic conditions that have led to the explosive growth of the Fintech sector warrant the adoption of stricter, more robust data security requirements for Fintech companies.[4]

As described in further detail below:

- Fintech has expanded significantly in recent years into consumer payment and other services traditionally provided by banks. Since the adoption of the Safeguards Rule, the Fintech industry has developed and grown rapidly, in parallel with, and on the foundation of, innovations in the technology and financial sectors. This has included an expansion, especially by alternative payment providers ("APPs") and data aggregators, into services traditionally offered exclusively by banks. These

---

3 *See Fin[t]ech Series: Crowdfunding & Peer-to-Peer Payments*, FTC (Oct. 26, 2016), https://www.ftc.gov/news-events/events-calendar/2016/10/fintech-series-crowdfunding-peer-peer-payments.

4 In the course of responding to this question, this letter also addresses, in whole or in part, a number of other questions posed by the FTC, including questions: (i) A.3 ("What modifications, if any, should be made to the Rule to increase its benefits to consumers"); (ii) B.1 ("Should the elements of an information security program include a response plan in the event of a breach that affects the security, integrity, or confidentiality of customer information? Why or why not? If so, what should such a plan contain?); and (iii) B.2 ("Should the Rule be modified to include more specific and prescriptive requirements for information security plans? Why or why not? If so, what requirements should be included and what sources should they draw from?").

companies hold vast amounts of consumer financial data, and thereby pose a risk to the security of consumer financial information, as well as to the safety and soundness of the financial system. In response to these developments, both Congress and regulators, including the FTC, have recently begun to express a growing interest in regulating Fintech companies in a number of areas, including data security and privacy.

- Although increasingly engaged in many of the same activities, Fintech providers are subject to significantly less stringent regulatory requirements concerning data security and privacy than are banks. While both banks and many Fintech companies are subject to the Gramm-Leach-Bliley Act's ("GLBA") data security requirements, banks are subject to detailed regulations and guidance documents promulgated by the financial regulatory agencies that make up the FFIEC, while Fintech companies are subject only to the FTC's very general requirements in the Safeguards Rule. Key differences between the two sets of requirements include not only the level of detail, but also standards regarding board and management involvement, employee background checks, vendor oversight, authentication, and incident response programs. Many Fintech companies also dramatically limit their liability for compromises of customer financial information and/or unauthorized transactions in the terms and conditions to which they bind consumers. The lighter substantive regulatory requirements Fintech companies face, combined with contractual limits on liability, result in materially weaker data security protections for consumers' financial information held by Fintech companies as compared to the protections in place for banks when both are engaged in the same activities.

- The Clearing House recommends enhancing the substantive regulatory requirements applicable to Fintech companies, perhaps through a two-tier regulatory structure. Banks and Fintech companies engaging in functionally similar activities and possessing comparable types and volumes of consumer data should be subject to similar, heightened regulatory regimes. While the Safeguards Rule's current high-level approach may be appropriate for "mom and pop shops" and other non-bank financial institutions engaging in lower risk businesses, this same approach is simply not sufficient for Fintech companies, such as APPs and data aggregators, and the risks posed by their data collection and processing activities. A similar regulatory standard for banks and these types of Fintech companies is critical to ensuring that consumer financial information is protected consistently, regardless of the consumer's choice of platform, and to protect the safety and soundness of the financial system. At minimum, the FTC should issue enhanced rules that expressly address the key gaps between the Safeguards Rule and the rules applicable to banks. These enhanced rules could either be limited to certain categories of Fintech companies, or apply more broadly to all companies subject to the FTC's jurisdiction.

II. In Recent Years, The Fintech Sector Has Grown and Expanded into Traditional Bank Services.

In recent years, the Fintech industry has evolved rapidly, in parallel with, and on the foundation of, innovations in the technology and financial sectors. This has included an expansion of the services offered by Fintech companies into many consumer payment and other services traditionally provided by banks, especially by APPs, including peer-to-peer ("P2P") payment services, and data aggregators. Aggregators often gain direct access to consumers' financial accounts (including through the collection, storage, and use of financial account credentials).[5]

A. Alternative Payment Providers

Many Fintech companies offer consumers alternative payment solutions, including new digital means to pay merchants, exchange money with friends, and use their wallets in other contexts, with Fintech companies providing payment services that had traditionally been provided by banks. These companies range from large tech companies, such as Apple Pay, Android Pay, and Facebook Messenger;[6] 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,[7] P2P money transfer services PayPal and Venmo,[8] entities that act as a

---

5 Financial account credentials include bank-issued consumer account passwords and account IDs, as well as the consumer's pre-arranged responses to the banks' security questions. This information, if compromised, could be used by criminals in an attempt to defeat banks' authentication protocols.

6 Apple Pay is a mobile payment service that lets Apple mobile devices make payments by aggregating, digitizing, and replacing magnetic stripe cards. Apple Pay, http://www.apple.com/apple-pay/. Android Pay 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. https://www.android.com/pay/. 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/.

7 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 Register, https://squareup.com/register; Square Stand, https://squareup.com/stand; 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. LevelUp, https://www.thelevelup.com/. 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/.

8 PayPal is an e-commerce business (owned by eBay) 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

front-end to the ACH rail such as Knox Payments,[9] and application program interfaces ("APIs") Stripe and Plaid;[10] to a number of earlier-stage startups seeking to introduce payment innovations and asking consumers to entrust their money to them.

The alternative payments industry has seen tremendous growth over the last few years. For example:

- **Growth of PayPal.** In Q1 2010, PayPal processed a net total payment volume of just over $20 billion,[11] and has now more than quadrupled, reaching $81 billion in Q4 2015.[12] In that same period, mobile payments on PayPal grew from $750 *million* annually in 2010 to $66 *billion* in 2015.[13]

- **Growth of P2P market.** In 2010, only 4% of web-connected adults used P2P mobile payments,[14] 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.[15] In July 2013, just over a year after its public launch, Venmo's user figures were reportedly

---

cards. Venmo (which was 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.

9 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/.

10 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/.

11 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/.

12 Statista, *PayPal's total payment volume from 1st quarter 2014 to 2nd quarter 2016 (in billion U.S. dollars)*, http://www.statista.com/statistics/277841/paypals-total-payment-volume/.

13 Statista, *PayPal's annual mobile payment volume from 2008 to 2015(in million U.S. dollars)*, http://www.statista.com/statistics/277819/paypals-annual-mobile-payment-volume/.

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

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

growing at a rate of 15% every month.[16] The mobile P2P payment market totaled a reported $5.2 billion in 2014[17] and is forecast to reach $27.05 billion this year.[18] During her opening remarks at the FTC's recent Crowdfunding and P2P payments event, FTC Commissioner McSweeny described P2P as "hugely popular," citing a 2015 survey saying that 46% of consumers have used mobile applications to make P2P payments, with 27% doing so at least monthly.[19]

- **Growth of alternative payments and e-wallets.** In 2015, it was estimated that alternative payments accounted for 51 % of market share, passing the share of card payments for the first time.[20] The same report predicted that e-wallets will surpass credit cards in the global e-commerce market by 2019, estimating that e-wallets will account for 27 % of the market, while credit cards will account for 24 %.[21] Another study estimates that contactless payments, which totaled $4.3 billion in 2013, will grow to $9.9 billion in 2018.[22]

- **Growth of mobile payments generally.** In 2010, $16 billion in transactions were processed as mobile payments.[23] This year, estimates show that mobile payments are expected to reach $75 billion, and are expected to reach $503 billion by 2020.[24] In

---

16 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/.

17 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.

18 Sarah Silbert, *How Mobile Payments Will Grow in 2016*, Fortune (Oct. 29, 2015), http://fortune.com/2015/10/29/mobile-payments-grow-2016/.

19 *See Fin[t]ech Series: Crowdfunding & Peer-to-Peer Payments*, FTC.

20 WorldPay, *Digital Payments Market to Leave Growing Pains Behind in 2016*, PR Newswire (Dec. 2, 2015), http://www.prnewswire.com/news-releases/digital-payments-market-to-leave-growing-pains-behind-in-2016-559949561.html.

21 *Id.*

22 Capgemini and Royal Bank of Scotland, *World Payments Report 2016*, at 27.

23 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.

24 Evan Bakker, *The Mobile Payments Report: Market Forecasts, Consumer Trends, and the Barriers and Benefits that will Influence Adoption*, Business Insider (June 3, 2016), http://www.businessinsider.com/the-mobile-payments-report-market-forecasts-consumer-trends-and-the-barriers-and-benefits-that-will-influence-adoption-2016-5.

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.[25] Another study this year found that one-third of retail banking customers world-wide make a mobile payment or use mobile banking services every week.[26] Current forecasts expect 56% of the consumer populations to do so by the end of 2020.[27]

B. Data Aggregators

Another group of Fintech companies that collect and process large volumes of sensitive financial information are data aggregators, which often use consumer financial account login information to retrieve and aggregate data across traditional financial institutions for consumer budgeting, data verification, and bill payment/funds transfers. Perhaps the most well-known data aggregator is Intuit's Mint. In just two years after its launch in 2007, Mint reached 1.5 million users nationwide,[28] and this year Mint.com has over 20 million users.[29] Given the popularity of Mint and other similar applications, consumers are going to continue to demand these aggregation services, requiring attention to the data security risks at issue.

Data aggregators generally access a consumer's bank account using the consumer's bank-issued log-in credentials, such as their username and password.[30] Data aggregators use this information to collect data from the consumer's financial accounts, typically by "screen scraping," though some collect data from banks through direct data feeds by agreement between the aggregator and the bank. Collection of consumer account data through bank-approved data

---

25 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.

26 Capgemini and Royal Bank of Scotland, *World Payments Report 2016*, at 14.

27 Evan Bakker, The Mobile Payments Report: Market Forecasts, *Consumer Trends, and the Barriers and Benefits that will Influence Adoption*, Business Insider (June 3, 2016), http://www.businessinsider.com/the-mobile-payments-report-market-forecasts-consumer-trends-and-the-barriers-and-benefits-that-will-influence-adoption-2016-5.

28 Justin Kuepper, *Top Problem with Financial Data Aggregation*, Investopedia, http://www.investopedia.com/articles/financial-advisors/021216/top-problems-financial-data-aggregation.asp.

29 Kim Tracy Prince, Mintlife Blog, *Mint by the Numbers: Which User Are You?*, (Apr. 6, 2016), https://blog.mint.com/credit/mint-by-the-numbers-which-user-are-you-040616/.

30 Veronica Dagher, *Consumers' Finance Data Still Flows at Aggregation Services for Financial Advisers*, The Wall Street Journal (Nov. 11, 2015).

feeds is more common when the bank has commissioned the aggregation services or when the bank has contractually agreed to such access in exchange for access controls and limitations.[31]

Under the latter model, banks are providing oversight to the aggregator as part of the bank's own compliance obligations. As such, these bank partnership arrangements frequently are secured through technologies such as encryption or tokenization, an approach previously endorsed by the Office of the Comptroller of the Currency ("OCC").[32] As a practical matter, this means that banks will generally share data through these feeds only when the banks feel comfortable that the recipient aggregator employs sufficient security controls, recognizing that the bank will likely be held liable for their service providers; by contrast, the least secure aggregators, subject to no bank oversight, will use the "surprisingly crude" and "insecure" screen scraping method.[33] The result is an ever-widening gap in the security of consumer data as between the aggregators partnering with banks and those that do not.

The three main types of data aggregation services are account aggregation, data verifications, and funds transfers.

- **Account Aggregation**. Account aggregation gives the consumer the ability to use a single sign-on to the data aggregator's website or application to gain access to information about all of the consumer's accounts registered with the data aggregator. Account aggregation includes two different business models: Business-to-Consumer ("B2C") and Business-to-Business-to-Consumer ("B2B2C"). Under the B2C model, the data aggregator collects bank-issued log-in credentials from the consumer and pulls data from the consumer's relevant financial accounts. Under the B2B2C model, the data aggregator (the "Primary Aggregator) provides data aggregation services to business customers ("Secondary Aggregators"), and the Secondary Aggregators, in turn, provide services to consumers. Under both models, the consumer only needs to use one set of log-in credentials to access the data aggregator's site, rather than the log-in information for each of the underlying accounts, so that consumers can view their financial information in one place.

- **Data Verification**. Some data aggregators collect the consumer's bank-issued log-in credentials for the purpose of verifying that a particular bank account is actually owned by the consumer, and that the account has a sufficient balance to permit payment to a merchant-payee in a requested purchase transaction. This service is typically provided to facilitate the processing of ACH payments by the merchant-

---

31 For example, Yodlee notes in its 2014 Form 10-K that it collects data for its data aggregation platform from 14,000 sources, and "75% of this data is collected through structured feeds from our [financial institution ("FI")] customers and other FIs." Item 1, Yodlee 2014 Form 10-K.

32 For banks that provide aggregation services through a third-party service provider, "[t]he OCC encourages the use of data feed arrangements where practical." OCC Bulletin 2001-12, 5 (Feb. 28, 2001).

33 Danny Vinik, *Can Washington control high-tech lending?*, Politico (Sept. 28, 2016).

payee. Following verification, credentials are typically not retained by the data aggregator, as service provider to the merchant-payee, though this is not always clear from publicly-available information, and may depend on whether the data aggregator providing the data verification services is doing so as a Primary or Secondary Aggregator.

- **Funds Transfers**. Some data aggregators use the consumer's bank-issued log-in credentials to present the consumer with a funds transfer screen, designed to collect the required information to initiate a funds transfer at a bank. For example, Mint offers a bill payment service through which a consumer enters log-in credentials, and the consumer's various bills are displayed in a single location. The consumer can then initiate a payment through Mint from a bank account aggregated at Mint to a biller aggregated at Mint.

Regardless of the services provided, a breach at a data aggregator that compromises consumers' bank-issued log-in credentials could have serious consequences for both consumers and the broader financial system.

C. Data Security Risks

Along with Fintech companies' rapid growth have come data security risks and lapses. For example, as recently as the end of 2014, there were reports of various security vulnerabilities in PayPal, a veteran payments 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."[34]

Venmo has also been the subject of criticism, following a May 2015 article which documented user complaints about fraud in the service tied to security failures.[35] The article highlighted the fact that key account information could 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.[36] This is a fairly basic security mistake that

---

34 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.

35 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.

36 *Id.* The article indicated that it was the user's bank, not Venmo, that alerted the user to the pending transfer.

financial regulators would not stand for when it comes to regulated banks. In fact, in the Federal FFIEC 2011 guidance *Supplement to Authentication in an Internet Banking Environment*, the FFIEC made 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 any one control, including through the use of "enhanced control over changes to account maintenance activities performed by customers."[37] This would presumably include changes to an account's associated email address. Notably, PayPal (now the owner of Venmo) disclosed in a recent SEC filing that it has received a CID from the FTC regarding Venmo, perhaps indicating FTC recognition of the need for increased oversight of this sector.[38]

In another example of an APP security lapse, Starbucks acknowledged last May that criminals had been siphoning money away from victims' credit cards, bank accounts, and PayPal accounts through their Starbucks cards.[39] It denied that the recent compromises were the result of a cybersecurity breach,[40] 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.[41] 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.[42] 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.[43] These lapses are particularly striking, as the Starbucks application is "viewed by payments analysts and

---

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

38 PayPal, Form 10-Q at 23 (April 28, 2016), https://investor.paypal-corp.com/secfiling.cfm?filingID=1633917-16-161&CIK=1633917.

39 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/.

40 Sullivan, *supra.*

41 *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/.

42 FFIEC, *Supplement to Authentication in an Internet Banking Environment.*

43 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/.

industry trade reports as an *example of successful implementation* of a closed-loop mobile payment model."[44]

These security shortcomings are particularly significant because, as noted by Matt Van Buskirk, former Director of Compliance at P2P company Circle, during the FTC's recent Fintech forum panel on P2P payments, every new Fintech company is likely to be targeted by sophisticated international criminals who may assume that new companies do not have advanced security measures in place.[45] Further, APPs collect a significant amount of customer data, which is at risk of being stolen by hackers if insufficient security precautions are put in place. During the early pilot stages of APP CurrentC,[46] for example, 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.[47]

Data aggregators also pose security risks, particularly in light of the fact that they store information (including authentication information) and/or provide direct access for executing financial transactions, across multiple financial accounts. Thus, whereas a data breach at a financial institution could pose a risk to consumers' financial accounts at that particular financial institution, a breach involving a data aggregator risks a simultaneous compromise of *all* of its customers' financial accounts, irrespective of the data security controls and protections that may be in place at the underlying financial institutions.

For example, a data breach occurring at an account aggregator can result in the unauthorized access of personal information of a single consumer or an aggregator's entire consumer base. The risk of data security breaches and resulting unauthorized transfers from consumer accounts exists in both account aggregator models, and may, in fact, be more pronounced in the B2B2C model than in the B2C model in light of the number of different entities involved. These risks may be mitigated when there is an arrangement between data aggregator and the bank pursuant to which the bank plays a more active role in managing the access to its systems by the data aggregator because the bank's vendor oversight obligations effectively require banks to impose their own stricter data security regulatory obligations on the vendor aggregator by contract. But where no such relationship exists, data aggregators are currently subject only to the limited regime of the Safeguards Rule, as explained more fully below. Data verification services pose similar risks to consumers, as log-in credentials are

---

44 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), http://www.bostonfed.org/bankinfo/payment-strategies/publications/2013/summary-of-mpiw-meeting-june-2013.pdf (emphasis added).

45 *See Fin[t]ech Series: Crowdfunding & Peer-to-Peer Payments*, FTC.

46 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/.

47 *Id.*

shared electronically by the consumer with the data aggregator, and it is unclear whether such data is retained after verification or otherwise properly disposed.

Data aggregators that also provide funds transfer services pose a different, and perhaps more direct risk to consumers than other data aggregators, with risks more akin to those in APPs. In addition to collecting, displaying and storing consumers' aggregated financial data, such services facilitate consumers' ability to process electronic funds transfers from their bank account(s) through the funds transfer services' site. This raises the possibility not only of consumer information being stolen from these companies' networks, but also of account takeover, resulting in unauthorized electronic funds transfers.

D. Increased Regulatory and Congressional Interest

Recognizing the growing role of Fintech, federal regulators have demonstrated an increased interest in the sector over the past year, including Fintech's implications for consumer protections as well as the safety and soundness of the financial system. This includes the FTC's Fintech Forum series, which started with a marketplace lending forum in June, and covered crowdfunding and P2P payments just last month.[48] At the June forum, data security was among a number of consumer protection issues that the FTC discussed with industry leaders and consumer advocates. The FTC has noted that "marketplace lending participants should keep in mind the existing legal constraints and disclosure of sensitive information" and that "market participants must also keep in mind consumer privacy protections under Section 5 [of the FTC Act] and the Privacy and Safeguards Rules of the [Gramm-Leach-Bliley] Act, and take appropriate steps to secure consumer data."[49] Indeed, at the Forum, the FTC highlighted its 2015 "Start with Security" guidance,[50] which it said should serve as a primer for Fintech companies.

A number of other regulators and congressional leaders have shown increased interest in the Fintech sector as well, recognizing the expanding role played by Fintech and the need to properly account for this role in federal regulatory efforts. For example:

- Last winter, the Federal Deposit Insurance Corporation ("FDIC") published supervisory insights focused on a framework for cybersecurity and a review of marketplace lending.[51]

---

48 Duane Pozza and Helen Wong, *Fin[t]ech Forum: A Closer Look at Marketplace Lending*, FTC (Aug. 3, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/fintech-forum-closer-look-marketplace-lending; *FTC to Host Fin[t]ech Forum on Crowdfunding and Peer-to-Peer Payments on Oct. 26*, FTC (Aug, 3, 2016), https://www.ftc.gov/news-events/press-releases/2016/08/ftc-host-fintech-forum-crowdfunding-peer-peer-payments-oct-26.

49 Duane Pozza and Helen Wong, *Fin[t]ech Forum: A Closer Look at Marketplace Lending.*

50 FTC, Start with Security: A Guide for Business (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

- In its 2016 Annual Report, the Financial Stability Oversight Council ("FSOC") listed financial innovation as a regulatory priority.[52] The FSOC has called for regulators to "monitor and evaluate the implications of how new products and practices affect regulated entities and financial markets, and to assess whether they could pose risks to financial stability."[53] The FSOC also said that financial innovations "merit special attention from financial regulators who must be vigilant to ensure that new products and practices do not blunt the effectiveness of existing regulations…,"[54] adding that "policies to protect consumers should be reviewed on an ongoing basis to assess the appropriate treatment of new products."[55]

- During the spring and summer of 2016, the OCC issued a white paper and held a forum on responsible innovation.[56] The OCC subsequently announced that it was examining its legal authority to offer a limited-purpose charter for Fintech firms.[57] A few weeks ago, the OCC released its Recommendations and Decisions for Implementing a Responsible Innovation Framework.[58] Among other things, the OCC report recommended that the OCC expand recruiting to ensure it broadens the skills of its employees, including seeking to recruit specialists in cybersecurity.[59] The OCC also announced that it was opening an Office of Innovation, focused on helping banks and other companies develop Fintech products and services in a manner that both complies with federal law and implements safety and consumer protection measures.

---

51 FDIC Supervisory Insights (Winter 2015), https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin15/SI_Winter2015.pdf.

52 FSOC 2016 Annual Report (June 2016), https://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/FSOC%202016%20Annual%20Report.pdf.

53 *Id.*, at 18.

54 *Id.*, at 126.

55 *Id.*, at 18.

56 OCC, *Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective* (March 2016), http://www.occ.gov/publications/publications-by-type/other-publications-reports/pub-responsible-innovation-banking-system-occ-perspective.pdf.

57 *OCC Examining Possibility of Limited-Purpose Fintech Charter*, ABA Banking Journal (June 14, 2016), http://bankingjournal.aba.com/2016/06/occ-examining-possibility-of-limited-purpose-fintech-charter/.

58 OCC, *Recommendations and Decisions for Implementing a Responsible Innovation Framework* (Oct. 2016), https://www.occ.gov/topics/bank-operations/innovation/recommendations-decisions-for-implementing-a-responsible-innovation-framework.pdf.

59 *Id.* at 10.

- The Treasury Department issued white paper in May 2016 focused on Fintech.[60]

- Also in May, 12 Members of the House of Representatives, led by Representatives Patrick McHenry (R-NC) and Randy Hultgren (D-CO) wrote a letter to the Government Accountability Office, inquiring about the current "regulatory structure" between banks and Fintech companies.[61]

- At the state level, on May 20, 2016, Texas Attorney General Ken Paxton announced that his office had entered into a settlement with PayPal regarding Venmo's privacy and security practices.[62] Attorney General Paxton alleged that Venmo had violated the Texas Deceptive Trade Practices Act, and required the company (1) to improve disclosures on the application regarding privacy and security; (2) to better inform users of the safeguards available on the application; and (3) to ensure consumers understand who will be able to view their transaction information.[63]

- In June, the White House held a stakeholders meeting on Fintech, including representatives from traditional financial services companies, Fintech start-ups, investors, regulators, and policy experts, to discuss a number of issues related to Fintech, including cybersecurity and big data.[64]

- In July, Senators Sherrod Brown (D-OH) and Jeff Merkley (D-OR) sent a letter to the heads of the Federal Reserve Board, OCC, FDIC, National Credit Union Association, and Consumer Financial Protection Bureau ("CFPB"), requesting answers to specific questions regarding consumer protections applicable to Fintech companies, and steps that each agency is taking to ensure effective oversight, "as Congress considers its role in overseeing [F]intech and its impact on American consumers."[65]

---

60 U.S. Department of the Treasury, *Opportunities and Challenges in Online Marketplace Lending* (May 10, 2016), https://www.treasury.gov/connect/blog/Documents/Opportunities_and_Challenges_in_Online_Marketplace_Lending_white_paper.pdf.

61 Letter from Representative Patrick McHenry et al. to Gene L. Dodaro, Comptroller General of the United States (May 24, 2016).

62 Press Release, Attorney General of Texas, Attorney General Ken Paxton Announces Agreement to Protect Consumers; Reform Privacy and Security Practices with PayPal (May 20, 2016), https://texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-announces-agreement-to-protect-consumers.

63 *Id.*

64 Adrienne Harris, Special Assistant to the President for Economic Policy, *The Future of Finance is Now*, White House Blog (June 10, 2016, 6:00 PM), https://www.whitehouse.gov/blog/2016/06/10/future-finance-now.

- Reflecting growing congressional interest in Fintech, in September 2016, the Congressional Research Service published a report on Fintech in consumer and small-business lending.[66]

- On October 5, 2016, the CFPB published its final rule requiring certain disclosures and consumer protections for prepaid accounts. Both mobile wallets and P2P transfer services are specifically included under the definition of "prepaid account" and are subject to the rule.[67] While the rule, which will become effective in October 2017, does not impose any requirements on these companies to implement data security controls, it does exhibit the increasing regulator interest in bringing Fintech companies under a regulatory framework that addresses these developing technologies.

- On November 14, 2016, the Securities and Exchange Commission ("SEC") will host a forum "to discuss [Fintech] innovation in the financial services industry and its impact on investors."[68]

While not all of this regulatory and congressional interest has focused directly on APPs and data aggregators, they typically present even greater security concerns because of their access to bank platforms and rails and their collection and use of sensitive consumer financial information for their operations.

III. Fintech Payment Providers Hold Vast Amounts of Consumer Data, But Are Subject to Only Limited Regulatory Requirements.

Fintech companies often possess large amounts of consumer financial information, and often have direct access to consumer bank accounts or account log-in information. Despite this level of access, these companies are holding this information under loose regulatory regimes and provide such services under contractual terms and conditions that severely limit the companies' liability without offering appropriate protection to consumers. Without more stringent, mandated security standards, the amount of data at risk in these companies' possession will

---

65 Letter from Senator Sherrod Brown and Senator Jeff Merkley to Janet Yellen, Chair, Board of Governors, Federal Reserve System, et al. (July 21, 2016), http://www.brown.senate.gov/download/fintech-letter_-2016-07-21.

66 David W. Perkins, Cong. Research Serv., R44614, *Marketplace Lending: Fintech in Consumer and Small-Business Lending* (2016).

67 Consumer Financial Protection Bureau ("CFPB"), Docket No. CFPB-2014-0031, *Prepaid Accounts under the Electronic Fund Transfer Act (Regulation E) and the Truth In Lending Act (Regulation Z)*, (Oct. 5, 2016), http://files.consumerfinance.gov/f/documents/20161005_cfpb_Final_Rule_Prepaid_Accounts.pdf.

68 *SEC to Hold Forum to Discuss Fintech Innovation in the Financial Services Industry*, Press Release 2016-195, (Sep. 27, 2016), https://www.sec.gov/news/pressrelease/2016-195.html.

continue to grow, resulting in increased risk both to consumers and to the safety and soundness of the financial system more broadly.

A. Fintech Companies Subject to the FTC Safeguards Rule are Subject to Dramatically Lighter Regulatory Requirements than Banks While Engaged in Similar Activities.

While both banks and many Fintech companies are subject to the data security requirements established in the GLBA, the two groups operate under quite different sets of implementing regulations and regulatory guidance. Banks are subject to the more detailed and demanding standards adopted jointly by the federal financial regulatory agencies, while those Fintech companies covered by the GLBA are subject to the more general Safeguards Rule promulgated by the FTC. The resulting lighter substantive requirements, combined with decreased odds of enforcement actions and less prospect of substantial monetary sanctions for violations, ultimately results in weaker data security protections for consumers' financial information when it is held by Fintech companies.

1. 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* ("Interagency Guidelines").[69] 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.[70] 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.[71]

Financial institutions' information security programs must include six components: (i) board of directors' involvement, including at least annual reporting to the board; (ii) risk assessment; (iii) risk management and control; (iv) oversight of service providers; (v) an incident response program; and (vi) periodic updating. The Interagency Guidelines provide detailed requirements for each of these six components.

---

69 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.

70 *Id.* § II.A.

71 *Id.* § II.B.

The Interagency Guidelines have been further supplemented by various guidance documents issued by the FFIEC member agencies. These include the FFIEC's Information Technology Examination Handbook, especially its Information Security, Outsourcing Technology Services, and Supervising Technology Service Providers booklets[72] as well as topical bulletins that include information security components,[73] and other guidance documents, such as the Cybersecurity Assessment Tool released last year.[74] The IT Examination Handbook's Information Security booklet alone contains nearly 90 pages of detailed security guidance, including information on implementation of specific security controls (ranging from remote access to encryption key management) and security monitoring.[75]

2. The Commission's Safeguards Rule

While most Fintech companies are likely subject to the GLBA's data security requirements,[76] they do not have to follow the Interagency Guidelines. Instead, they are subject to the more general requirements of the FTC's Safeguards Rule.[77] 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 provides only the most general requirements with covered institutions being required to implement a written information security program containing

---

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

73 *See, e.g.*, FFIEC, *Joint Statement on Cybersecurity of Interbank Messaging and Wholesale Payment Networks*, http://www.ffiec.gov/press/PDF/Cybersecurity_of_IMWPN.pdf; FFIEC, *Joint Statement on Cyber Attacks Involving Extortion*, http://www.ffiec.gov/press/PDF/FFIEC_Joint_Statement_Cyber_Attacks_Involving_Extortion_-_Interactive_Ve%20%20%20.pdf; *Risk Management Guidance*, OCC Bulletin 2013-29 (Oct. 30, 2013), 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.*

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

75 FFIEC, *Information Security* (September 2016), http://www.ffiec.gov/press/PDF/FFIEC_IT_Handbook_Information_Security_Booklet.pdf.

76 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" and "[p]roviding financial . . . or economic advisory services").

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

administrative, technical, and physical safeguards "appropriate" to the company's size, complexity, activities, and maintenance of sensitive customer information.[78] The Safeguards Rule outlines five very basic required elements for developing, implementing, and maintaining an information security program: (i) designate an employee to coordinate the program; (ii) 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; (iii) design and implement information safeguards to control risks identified through regular assessments, and regularly test or monitor the effectiveness of key controls; (iv) oversee service providers, including taking reasonable steps to retain providers that are capable of maintaining appropriate safeguards and contractual provisions requiring such safeguards; and (v) 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.[79] Unlike in the Interagency Guidelines, the Safeguards Rule does not provide additional detail for these requirements.

3. Some Key Distinctions

The differences between the data security requirements imposed on banks by the Interagency Guidelines and those applicable to Fintech (and other) companies under the Safeguards Rule are numerous, even though the information held by banks and Fintech companies and risks attendant to each may be identical. Here we highlight six fundamental ones.

First, the difference in the level of detail between the two regimes has real material implications for types of data security precautions regulators can reasonably demand, and consumers should reasonably expect, from banks, on the one hand, as compared to non-bank Fintech companies, on the other. For example, a Fintech company subject to an investigation and/or potential enforcement action by the FTC may argue that there are no specific requirements for technical controls they are required to employ to control identified risks.[80] By contrast, no reasonable bank could argue that it is not required to consider specific access controls, encryption, segregation of duties, and other controls that are explicitly identified in the Interagency Guidelines.[81] 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.

---

78 *Id.* § 314.3(a).

79 *Id.* § 314.4.

80 *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.")

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

Second, the Interagency Guidelines require involvement from bank leadership at the highest level, including boards of directors and senior business management.[82] Under the Interagency Guidelines, 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.[83] By contrast, under the Safeguards Rule, Fintech companies can simply designate an employee to coordinate the information security program and train their employees, without having to involve their senior leadership. Particularly with rapidly growing start-up companies with small staffs yet large volumes of consumer financial information, the lack of a requirement for senior leadership involvement may well result in data security being deprioritized over growing the business's consumer base, ensuring a quick return on investment, and maximizing profit.

Third, recognizing the significant risk posed by insider threats, the Interagency Guidelines require banks to consider, and, if appropriate, adopt, 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.[84] 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.[85]

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 service providers and including data security requirements in service provider contracts (both of which are generally required by the Safeguards Rule as well[86]), the Interagency Guidelines require banks,

---

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

83 12 C.F.R. Part 30, App. B § III.A, F.

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

85 *See, e.g.*, Marc van Zadelhoff, *The Biggest Cybersecurity Threats Are Inside Your Company*, Harvard Business Review (Sept. 19, 2016), https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company.

86 16 C.F.R. § 314.4(d); 12 C.F.R. Part 30, App. B § III.D.1-2.

where indicated by their risk assessments, 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."[87] 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.[88] Under the Safeguards Rule, by contrast, Fintech companies are free from any express regulatory requirement mandating such ongoing vendor supervision.

While the FTC has used its enforcement authority under Section 5 of the FTC Act to require ongoing monitoring of vendor data security even outside of financial institutions and the GLBA Safeguards Rule, FTC enforcement under Section 5 of the FTC Act does not compensate for specific GLBA requirements, particularly because FTC enforcement of data security standards for financial institutions under its Section 5 jurisdiction has generally been used only to add additional charges in enforcement actions already being brought under the Safeguards Rule, rather than as a basis to bring an enforcement action where there was no specific Safeguards Rule violation.[89] Further, where the FTC has express rulemaking authority in the data security context, these standards should be at least as robust as standards set by the FTC via enforcement action and unofficial guidance.

More and more frequently, third-party service providers have been a vector for data breaches (either by an attacker accessing a company's networks via a direct service provider connection to the company's network, or by an attacker accessing a company's data processed or otherwise held by a third party). As such, when Fintech companies are not required to monitor the performance of their service providers, it puts those companies' customers at greater risk of having their information compromised. Further, where a Fintech company partners directly with a regulated bank as its service provider, the data security of those Fintech companies is monitored by the regulated bank under the bank's own GLBA obligations. However, these more stringent rules do not apply to Fintech companies acting independently.

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

---

87 *See*12 C.F.R. Part 30, App. B § III.D.3.

88 FFIEC, *Outsourcing Technology Services* (June 2004), http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_OutsourcingTechnologyServices.pdf.

89 *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).

procedures.[90] The FTC Safeguards Rule imposes no similar specific requirement on Fintech companies, 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 reported Fintech 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 FTC-regulated financial institutions. The gap is particularly shocking in light of the kinds of consumer financial information held by Fintech companies, particularly data aggregators' use of customer bank account log-in information, the breach of which could have serious implications for the safety and soundness of the financial system as a whole.

B. Fintech Companies' Consumer Terms and Conditions Often Limit Company Liability Without Protecting Consumers.

Perhaps reflecting the regulatory environment in which they operate, the terms and conditions for Fintech companies vary dramatically in terms of the liability protections for data compromise and/or unauthorized transactions through their platforms. This ultimately results in a remarkable lack of protection for consumers using these platforms.

For example, LevelUp requires that any unauthorized transaction be reported within 2 business days for a full reimbursement; otherwise the consumer is responsible for the fraudulent or unauthorized charges up to $500.[91] Terms such as these make it possible for the company to disclaim most liability, leaving consumers with little recourse against LevelUp.

Similarly, some data aggregators include strict liability limitations in their terms and conditions. For example, Intuit attempts to limit its liability "for any cause whatever" to $500,[92]

---

90 FFIEC, *Supplement to Authentication in an Internet Banking Environment.*

91 LevelUp User Terms of Service, Section 6.2, https://www.thelevelup.com/terms ("IF YOU FAIL TO NOTIFY LEVELUP OF A FRAUDULENT OR UNAUTHORIZED TRANSACTION WITHIN TWO (2) BUSINESS DAYS OF A TRANSACTION RECEIPT…YOU WILL BE RESPONSIBLE FOR THE FRAUDULENT OR UNAUTHORIZED CHARGES IN AN AMOUNT LIMITED TO THE LESSER OF: (I) $500; OR (II) THE SUM OF EITHER $50 OR THE AMOUNT OF THE FRAUDULENT USE DURING THE INITIAL TWO (2) DAYS (WHICHEVER IS LESS), AND THE SUM OF ALL FRAUDULENT OR UNAUTHORIZED ACTIVITY AFTER THE INITIAL TWO (2) DAYS PRIOR TO YOUR NOTIFICATION TO LEVELUP.")

92 Terms of Use, Mint, Section 17 (Limitation on Intuit's Liability), https://www.mint.com/terms ("...NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, INTUIT'S LIABILITY TO YOU FOR ANY CAUSE WHATEVER AND REGARDLESS OF THE FORM OF THE

and Personal Capital's Terms of Use state that the company's liability is limited to $100.[93] At Digit.co, a data aggregator that transfers consumer funds from checking into savings accounts, the Terms of Use expressly disclaim responsibility for any unauthorized or fraudulent transactions.[94]

The risk that these terms pose to consumers is only magnified by the limited data security requirements imposed on these companies by the Safeguards Rule, as these companies are free to implement only basic security controls, and then disclaim liability for resulting breach of consumer information and/or unauthorized transactions. This ensures little to no incentive for these companies to implement controls that rise to the level of those implemented by banks complying with the GLBA. At the same time, these companies possess large volumes of financial data akin to the financial data held by banks, often provide direct access to consumers' financial accounts, and may even facilitate transfers from consumers' financial accounts in the ordinary course. The combination of these factors has the potential to leave both consumers and the safety and soundness of the financial sector vulnerable to data security risks.

IV. The FTC Should Expand the Safeguards Rule, Potentially Through a Separate Rule Applicable to Higher Risk Companies, Including Fintech Companies.

Cybersecurity statutory mandates, regulatory frameworks, and administrative guidance are being tightened throughout the financial services sector in recognition of ever-increasing cyber security risks. Both Congress and regulators have recognized that the extent of regulatory requirements and guidance should be commensurate with the risks presented by covered entities' businesses. In assessing the risk profile for Fintech companies, it is important to remember that these companies do not just store personally identifiable information, but rather they collect, process, and handle particularly sensitive financial account information in the ordinary course and have actively sought to be engaged in such business. It is precisely because of both Congress' and the financial regulators' recognition of the heightened risks attached to unauthorized access to and disclosure of this sensitive financial account information, ranging from identity theft to account takeover, that lawmakers and regulators have imposed more stringent requirements upon banks through the GLBA and the Interagency Guidelines. Because

---

ACTION, WILL AT ALL TIMES BE LIMITED TO A MAXIMUM OF $500.00 (FIVE HUNDRED UNITED STATES DOLLARS).").

93 Terms of Use, Personal Capital, Section 16 (Limitation of Liability), https://www.personalcapital.com/content/terms-of-use/ ("TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE LIABILITY OF PERSONAL CAPITAL, ITS AFFILIATES, LICENSORS AND AGENTS TO YOU SHALL NOT EXCEED ONE HUNDRED U.S. DOLLARS ($100)...").

94 Terms of Use, Digit, https://digit.co/about/legal/terms-of-use ("EXCEPT AS OTHERWISE EXPRESSLY STATED IN THESE TERMS OR REQUIRED BY APPLICABLE LAW, WE ARE NOT RESPONSIBLE FOR ANY LOSSES ARISING OUT OF THE LOSS OR THEFT OF YOUR USER INFORMATION OR YOUR MOBILE DEVICE OR FROM UNAUTHORIZED OR FRAUDULENT TRANSACTIONS ASSOCIATED WITH YOUR BANK ACCOUNT OR YOUR DIGIT ACCOUNT.")

of similar risks, banks and Fintech companies engaging in functionally similar activities and possessing comparable types and volumes of consumer data must be subject to similar, heightened regulatory regimes. The continued failure to address gaps in the Safeguards Rule has significant implications for risks to consumers and to the safety and soundness of the financial system.

We appreciate that the Safeguards Rule was adopted in a different time and with an approach that may be appropriate for "mom and pop shops" and other non-bank financial institutions engaging in lower risk businesses. This same general approach, however, is simply not appropriate for Fintech companies, such as APPs and data aggregators, and the risks posed by their data collection and processing activities. A significantly more robust approach for Fintech companies is critical to ensuring that consumers enjoy consistent protection regardless of their choice of platform and to protect the safety and soundness of the financial system. In providing specific regulatory requirements for banks engaged in these activities, the regulators have recognized that certain higher-risk activities require a baseline set of controls that should be in place. Because of the similar risks posed to consumers and the safety and soundness of the financial system by a potential data security incident involving these types of Fintech companies, it is imperative that these companies be subject to regulatory requirements that provide far more specifics than the high-level approach taken under the current Safeguards Rule.

To ensure such protections, The Clearing House recommends enhancing the substantive regulatory requirements applicable to these entities. Notably, the substantive scope of the FTC's statutory rulemaking authority under the GLBA is the same as that of the prudential regulators, who, as described above, have issued significantly more detailed and expansive data security regulations under the GLBA. In light of its equivalent authority, as well as the changes in the industry and the risks to consumers and the safety and soundness of the financial system, the FTC should use its authority to adopt enhanced GLBA Safeguards Rules.

At minimum, these enhanced rules should include express regulatory requirements addressing the key gaps between the Interagency Guidelines and the Safeguards Rule identified above. The FTC can also look to its own enforcement actions and guidance, such as the "Start with Security" guidance, in determining specific security controls that should be mandated for these companies by regulation. These rules can either be limited to certain categories of Fintech companies (in which case the covered categories of institutions 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.

The Clearing House fully appreciates the FTC's desire to provide standards that are appropriate for both small and large entities covered by the Safeguards Rule. However, the financial services industry is simply not the same industry today as it was when the present regulations were issued. If having a single standard means that Fintech companies providing bank-like products and services are subject to overly lax security regulations, the current approach will lead to insufficient protections for both consumers and the financial market.

Furthermore, we believe that, in light of the risks posed by these entities, the FTC can articulate a clear, rational basis, sufficient to withstand a possible Administrative Procedures Act challenge, for establishing different regulatory requirements for different categories of entities subject to the FTC's GLBA authority. Simply put, Fintech companies that possess massive volumes of sensitive customer financial information, including direct financial account access and authentication information, and that knowingly and pervasively engage in activities traditionally performed by banks, should be required to comply with standards akin to the standards that actually apply to banks—standards that have been developed precisely to protect consumers from the data security risks facing entities engaged in these very types of services.

V. Conclusion

We appreciate this opportunity to comment on the Safeguards Rule, and hope that these points will be taken into consideration in the FTC's review of the regulations and any subsequent rulemaking process. The FTC, via its Safeguards Rule, has a unique opportunity to take action in an area of increased risk (both to consumers and the safety and soundness of the financial system) and of increased congressional and regulatory interest. If the FTC does not take advantage of this opportunity, for which it is uniquely situated in light of its experience in data security enforcement across sectors, one of the other interested regulators may step in to this space in its stead. If you have any questions, please contact the undersigned by phone at (336) 769-5314 or by email at Rob.Hunter@theclearinghouse.org.

Respectfully submitted,

/S/

Robert C. Hunter
Executive Managing Director & Deputy General Counsel
The Clearing House Association L.L.C.