# CFPB Weighs in on Data Security; Will Firms with Poor Security Be in the Crosshairs?

October 14, 2022

**Andrew E. Bigart**
Partner | + 1 202.344.4323 | aebigart@Venable.com

**Jeremy A. Grant**
Managing Director of Technology Business Strategy | + 1 202.344.4646 | jagrant@Venable.com

**Alexandra Megaris**
Partner | +1 212.370.6210 | amegaris@Venable.com

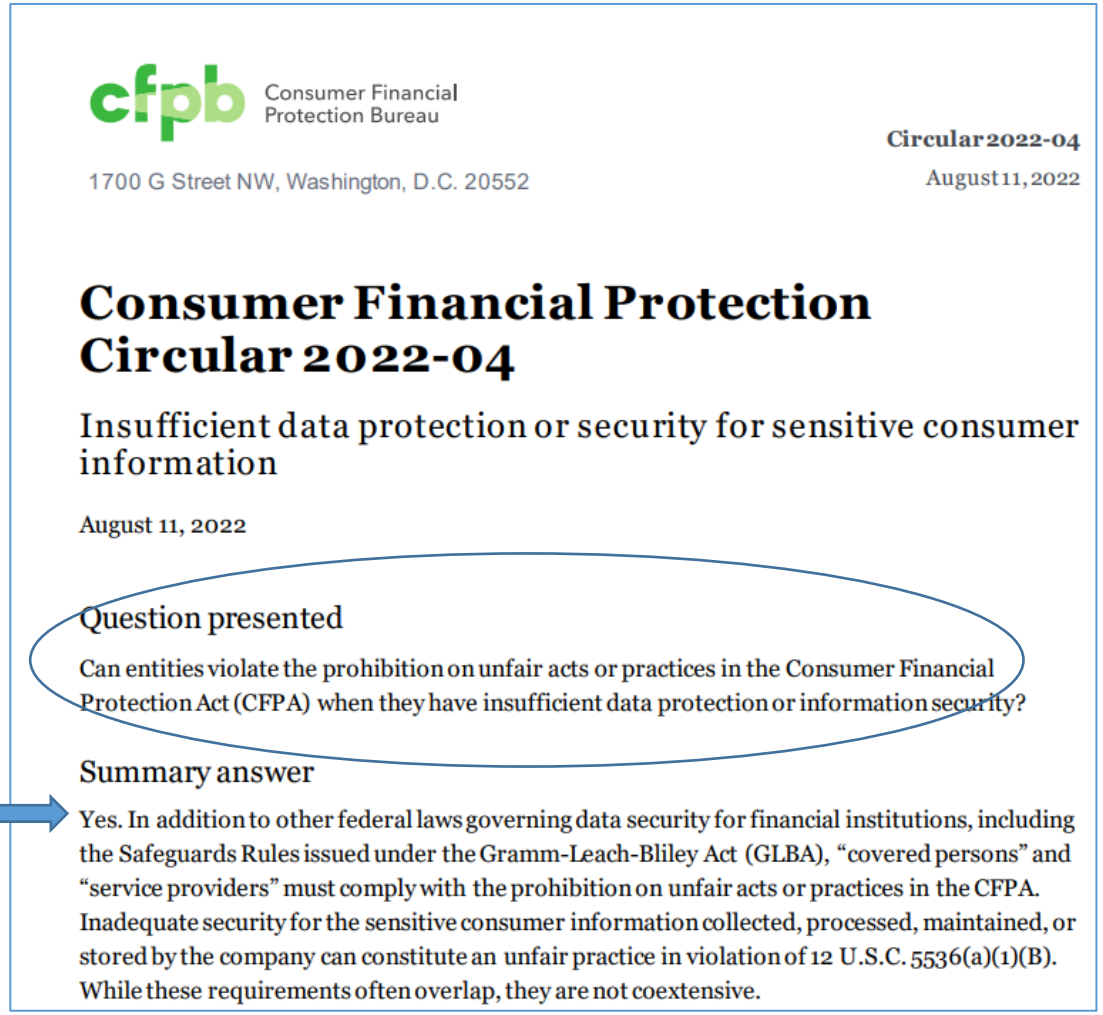
**Ross B. Nodurft**
Senior Director of Cybersecurity Services | +1 202.344.4403 | rbnodurft@Venable.com

VENABLE LLP

# Agenda

- Review of *CFPB Circular 2022-04: Insufficient data protection or security for sensitive consumer information*, issued August 2022
  - What is a Consumer Financial Protection Circular?
  - Existing legal framework for protecting consumer financial data on federal level
  - Data security lapses as potential UDAAP liability
- Multifactor authentication
- Password management
- Software updates
- Data security challenges presented by open banking, banking-as-a-service, and modern payments

# CFPB Issues Circular 2022-04 in August 2022



Consumer Financial Protection Bureau

1700 G Street NW, Washington, D.C. 20552

Circular 2022-04

August 11, 2022

## Consumer Financial Protection Circular 2022-04

### Insufficient data protection or security for sensitive consumer information

August 11, 2022

### Question presented

Can entities violate the prohibition on unfair acts or practices in the Consumer Financial Protection Act (CFPA) when they have insufficient data protection or information security?

### Summary answer

Yes. In addition to other federal laws governing data security for financial institutions, including the Safeguards Rules issued under the Gramm-Leach-Bliley Act (GLBA), "covered persons" and "service providers" must comply with the prohibition on unfair acts or practices in the CFPA. Inadequate security for the sensitive consumer information collected, processed, maintained, or stored by the company can constitute an unfair practice in violation of 12 U.S.C. 5536(a)(1)(B). While these requirements often overlap, they are not coextensive.

VENABLE LLP

# What Is a Consumer Financial Protection Circular and What Is Its Effect?

- Consumer Financial Protection Circulars are policy statements advising parties with authority to enforce federal consumer financial law, such as state attorneys general, state regulators, prudential regulators, FTC, and DOJ.
- Intended to promote consistency in approach across various enforcement agencies and to provide transparency to partner agencies regarding CFPB's approach when it engages in joint investigatory work.
- As general statements of policy under the Administrative Procedures Act, not subject to notice and comment like regulations. They are not supposed to impose any new legal requirement.

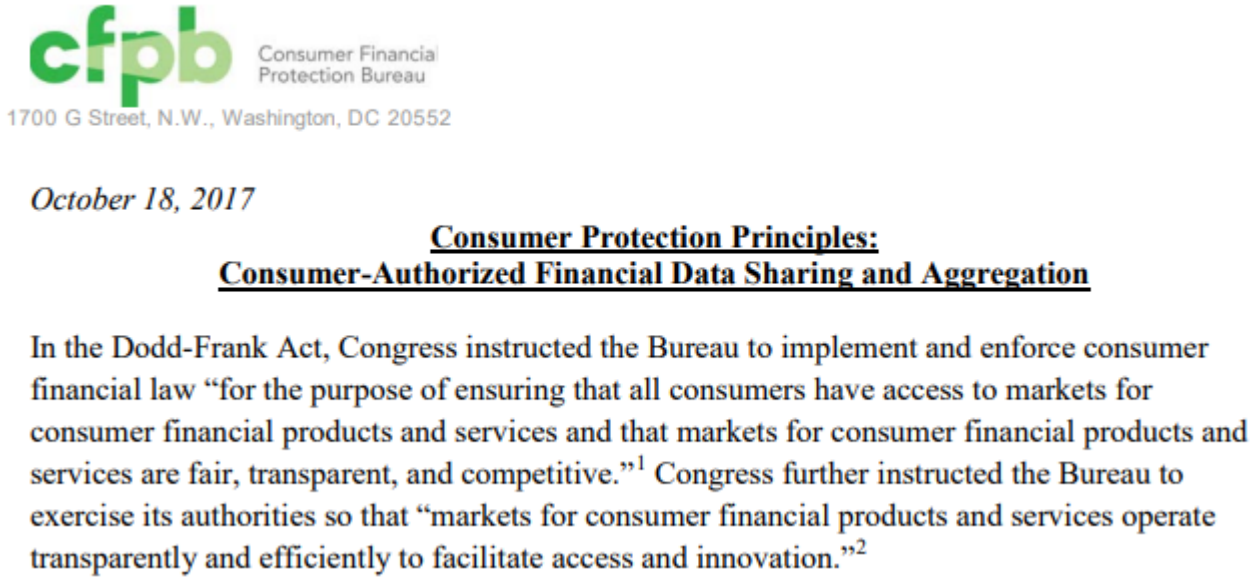
*"The CFPB Director is instructing CPFB staff as described herein, and the CFPB will then make final decisions on individual matters based on an assessment of the factual record, applicable law, and factors relevant to prosecutorial discretion."*

VENABLE LLP

# CFPB Principles for Consumer Permissioned Data Sharing

Previously, the CFPB published nine principles for consumer financial data

- access;
- data scope and usability;
- control and informed consent;
- authorizing payments;
- security;
- transparency of access;
- accuracy;
- ability to dispute and resolve unauthorized access; and
- efficient and effective accountability mechanisms.



cfpb Consumer Financial Protection Bureau

1700 G Street, N.W., Washington, DC 20552

*October 18, 2017*

**Consumer Protection Principles:**
**Consumer-Authorized Financial Data Sharing and Aggregation**

In the Dodd-Frank Act, Congress instructed the Bureau to implement and enforce consumer financial law "for the purpose of ensuring that all consumers have access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive."[1] Congress further instructed the Bureau to exercise its authorities so that "markets for consumer financial products and services operate transparently and efficiently to facilitate access and innovation."[2]

VENABLE LLP

# Key Players in Open Banking

**Data Holders:**

- Banks and credit unions that have established customer relationships and access to customer financial data. The CFPB refers to these institutions as “data holders,” because they hold information about the customer through their financial services relationship.

**Data Aggregator:**

- An entity that supports data users and/or data holders in enabling authorized data access.
- These entities access and transmit consumer financial data to data users pursuant to consumer authorization.

**Data User:**

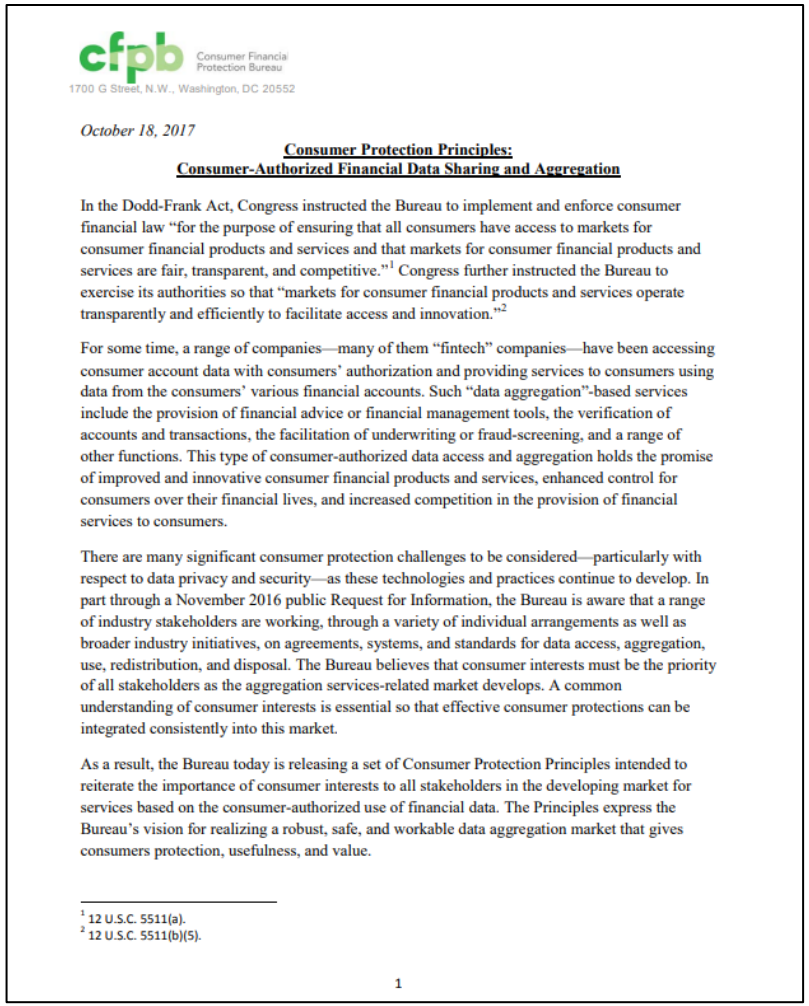
- Means a third party that uses consumer-authorized data access to provide either (1) products or services to the authorizing consumer or (2) services used by entities that provide products or services to the authorizing consumer.

# Section 1033 Rulemaking – Consumer-Authorized Financial Data Sharing and Aggregation

- Section 1033 of the Consumer Financial Protection Act requires a covered person to make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, to any series of transactions, or to the account, including costs, charges, and usage data.
- The information must be made available in an electronic form that is usable by consumers, but there is no duty for the covered person to maintain any records.
- Exceptions: A covered person may not be required by this section to make available to the consumer
  - any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors;
  - any information collected by the covered person for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct;
  - any information required to be kept confidential by any other provision of law; or
  - any information that the covered person cannot retrieve in the ordinary course of its business with respect to that information.

# Section 1033 Rulemaking Timeline

- November 22, 2016 – Request for Information
- November 18, 2017 – Principles Statement
- February 26, 2020 – Symposium
- October 22, 2020 – Advance Notice of Proposed Rulemaking
- February 4, 2021 – ANPR comments closed (99 comments received)
- July 9, 2021 – Executive Order (EO) encourages CFPB to commence rulemaking
- ***Present – Pre-Rule Stage – Final Rule?***



cfpb Consumer Financial Protection Bureau
1700 G Street, N.W., Washington, DC 20552

*October 18, 2017*

**Consumer Protection Principles:**
**Consumer-Authorized Financial Data Sharing and Aggregation**

In the Dodd-Frank Act, Congress instructed the Bureau to implement and enforce consumer financial law "for the purpose of ensuring that all consumers have access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive."[1] Congress further instructed the Bureau to exercise its authorities so that "markets for consumer financial products and services operate transparently and efficiently to facilitate access and innovation."[2]

For some time, a range of companies—many of them "fintech" companies—have been accessing consumer account data with consumers' authorization and providing services to consumers using data from the consumers' various financial accounts. Such "data aggregation"-based services include the provision of financial advice or financial management tools, the verification of accounts and transactions, the facilitation of underwriting or fraud-screening, and a range of other functions. This type of consumer-authorized data access and aggregation holds the promise of improved and innovative consumer financial products and services, enhanced control for consumers over their financial lives, and increased competition in the provision of financial services to consumers.

There are many significant consumer protection challenges to be considered—particularly with respect to data privacy and security—as these technologies and practices continue to develop. In part through a November 2016 public Request for Information, the Bureau is aware that a range of industry stakeholders are working, through a variety of individual arrangements as well as broader industry initiatives, on agreements, systems, and standards for data access, aggregation, use, redistribution, and disposal. The Bureau believes that consumer interests must be the priority of all stakeholders as the aggregation services-related market develops. A common understanding of consumer interests is essential so that effective consumer protections can be integrated consistently into this market.

As a result, the Bureau today is releasing a set of Consumer Protection Principles intended to reiterate the importance of consumer interests to all stakeholders in the developing market for services based on the consumer-authorized use of financial data. The Principles express the Bureau's vision for realizing a robust, safe, and workable data aggregation market that gives consumers protection, usefulness, and value.

[1] 12 U.S.C. 5511(a).
[2] 12 U.S.C. 5511(b)(5).

1

VENABLE LLP

# Existing Legal Framework for Consumer Financial Data – Nonbanks

## Gramm-Leach-Bliley Act and FTC Safeguards Rule

Applies to non-banking financial institutions, such as check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax preparers, courier services, and credit reporting agencies.

- Expands the scope of covered financial institutions to include "**finders**."
- Does not ***directly*** apply to service providers, but service providers should expect covered financial institutions to impose similar requirements by contract.

- As compared with the previous Safeguards Rule, the final rule imposes more detailed requirements for the development, establishment, and maintenance of information security programs.
  - These measures closely track recently enacted regulations by NYDFS, which enacted its own Cybersecurity Regulation in 2017.
- **Compliance Deadline:** October 27, 2022.

70272 Federal Register / Vol. 86, No. 234 / Thursday, December 9, 2021 / Rules and Regulations

FEDERAL TRADE COMMISSION

16 CFR Part 314

RIN 3084–AB35

**Standards for Safeguarding Customer Information**

**AGENCY:** Federal Trade Commission.

**ACTION:** Final rule.

**SUMMARY:** The Federal Trade Commission ("FTC" or "Commission") is issuing a final rule ("Final Rule") to amend the Standards for Safeguarding Customer Information ("Safeguards Rule" or "Rule"). The Final Rule contains five main modifications to the existing Rule. First, it adds provisions designed to provide covered financial institutions with more guidance on how to develop and implement specific aspects of an overall information security program, such as access controls, authentication, and encryption. Second, it adds provisions designed to improve the accountability of financial institutions' information security programs, such as by requiring periodic reports to boards of directors or governing bodies. Third, it exempts financial institutions that collect less customer information from certain requirements. Fourth, it expands the definition of "financial institution" to include entities engaged in activities the Federal Reserve Board determines to be incidental to financial activities. This change adds "finders"—companies that bring together buyers and sellers of a product or service—within the scope of the Rule. Finally, the Final Rule defines several terms and provides related examples in the Rule itself rather than incorporates them from the Privacy of Consumer Financial Information Rule ("Privacy Rule").

**DATES:**

*Effective date:* This rule is effective January 10, 2022.

*Applicability date:* The provisions set forth in § 314.5 are applicable beginning December 9, 2022.

**FOR FURTHER INFORMATION CONTACT:** David Lincicum (202–326–2773), Katherine McCarron (202–326–2333), or Robin Wetherill (202–326–2220), Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

**SUPPLEMENTARY INFORMATION:**

**I. Background**

Congress enacted the Gramm Leach Bliley Act ("GLB" or "GLBA") in 1999.[1] The GLBA provides a framework for regulating the privacy and data security practices of a broad range of financial institutions. Among other things, the GLBA requires financial institutions to provide customers with information about the institutions' privacy practices and about their opt-out rights, and to implement security safeguards for customer information.

Subtitle A of Title V of the GLBA required the Commission and other Federal agencies to establish standards for financial institutions relating to administrative, technical, and physical safeguards for certain information.[2] Pursuant to the Act's directive, the Commission promulgated the Safeguards Rule (16 CFR part 314) in 2002. The Safeguards Rule became effective on May 23, 2003.

The current Safeguards Rule requires a financial institution to develop, implement, and maintain a comprehensive information security program that consists of the administrative, technical, and physical safeguards the financial institution uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.[3] The information security program must be written in one or more readily accessible parts.[4] The safeguards set forth in the program must be appropriate to the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of any customer information at issue.[5] The safeguards must also be reasonably designed to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of the information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.[6]

In order to develop, implement, and maintain its information security program, a financial institution must 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.[7] The financial institution must then design and implement safeguards to control the risks identified through the risk assessment, and must regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.[8] The Rule also requires the financial institution to evaluate and adjust its information security program in light of the results of this testing and monitoring, any material changes in its operations or business arrangements, or any other circumstances it knows or has reason to know may have a material impact on its information security program.[9] The financial institution must also designate an employee or employees to coordinate the information security program.[10]

Finally, the current Safeguards Rule requires financial institutions to take reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for customer information and require those service providers by contract to implement and maintain such safeguards.[11]

**II. Regulatory Review of the Safeguards Rule**

On September 7, 2016, the Commission solicited comments on the Safeguards Rule as part of its periodic review of its rules and guides.[12] The Commission sought comment on a number of general issues, including the economic impact and benefits of the Rule; possible conflicts between the Rule and state, local, or other Federal laws or regulations; and the effect on the Rule of any technological, economic, or other industry changes. The Commission received 28 comments from individuals and entities representing a wide range of viewpoints.[13] Most commenters agreed there is a continuing need for the Rule and it benefits consumers and competition.[14]

On April 4, 2019, the Commission issued a notice of proposed rulemaking (NPRM) setting forth proposed amendments to the Safeguards Rule (the "Proposed Rule").[15] In response, the Commission received 49 comments from various interested parties

[1] Public Law 106–102, 113 Stat. 1338 (1999).

[2] See 15 U.S.C. 6801(b), 15 U.S.C. 6805(b)(2).

[3] 16 CFR 314.2(c).

[4] 16 CFR 314.3(a).

[5] 16 CFR 314.3(a), (b).

[6] 16 CFR 314.3(a), (b).

[7] 16 CFR 314.4(b).

[8] 16 CFR 314.4(c).

[9] 16 CFR 314.4(e).

[10] 16 CFR 314.4(a).

[11] 16 CFR 314.4(d).

[12] Safeguards Rule, Request for Comment, 81 FR 61632 (Sept. 7, 2016).

[13] The 28 public comments received prior to March 15, 2019, are posted at: https://www.ftc.gov/policy/public-comments/initiative-674.

[14] See, e.g., Mortgage Bankers Association (comment 34, NPRM); National Automobile Dealers Association (Comment 40, NPRM); Data & Marketing Association (comment 38, NPRM); Electronic Transactions Association (comment 24, NPRM); State Privacy & Security Coalition (comment 26, NPRM).

[15] FTC Notice of Proposed Rulemaking, 84 FR 13158 (April 4, 2019).

VENABLE LLP

# FTC Safeguards Final Rule: Key Changes

- Provides more specificity on how financial institutions should develop and implement aspects of an information security program. For instance, the rule requires:
  - Implementation and review of access controls;
  - Encryption of customer information in transit and at rest;
  - Development, implementation, and maintenance of information disposal practices; and
  - Adoption of change management procedures.
- Adds provisions designed to improve the accountability of financial institutions' information security programs.
  - Requires a financial institution to designate a "Qualified Individual" to be responsible for the program who regularly reports to the financial institution's board of directors or governing body.
- Exempts financial institutions that collect less customer information from certain requirements.

VENABLE LLP

# Existing Legal Framework for Consumer Financial Data – Banks

- The **Interagency Guidelines Establishing Information Security Standards** is a joint rule issued in February 2001 by OCC, Board of Reserves of Federal Reserve, FDIC, and Office of Thrift Supervision.
- Set forth standards pursuant to Sections 501 and 505 of the **Gramm-Leach-Bliley Act.** These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.
- The Guidelines apply to customer information maintained by or on behalf of bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisors), for which the Board has supervisory authority.

# Circular Declared That Data Security Practices—or Lack Thereof—Can Constitute a UDAAP

**In sum, per CFPB:**

- Financial service providers are subject to the Consumer Financial Protection Act, enforced by the CFPB, which generally prohibits "unfair" acts or practices.
- An unfair act or practice is one that:
  1. causes or is likely to cause substantial injury to consumers,
  2. is not reasonably avoidable by consumers, and
  3. is not outweighed by countervailing benefits to consumers or competition.
- In the Circular, CFPB announced, "When companies forgo reasonable cost-efficient measures to protect consumer data, like those identified below, the CFPB expects the risk of substantial injury to consumers will outweigh any purported countervailing benefits to consumers or competition."
- What are the "reasonable cost-efficient measures" that the CFPB identified?
  - Multi-factor
  - Password Management
  - Timely Software Updates

# Multi-Factor Authentication (MFA)

**Per CFPB:**

- "Multi-factor authentication (MFA) is a security enhancement that requires multiple credentials (factors) before an account can be accessed."
- "Factors fall into three categories: something you know, like a password; something you have, like a token; and something you are, like your fingerprint."
- "A common MFA setup is supplying both a password and a temporary numeric code in order to log in. Another MFA factor is the use of hardware identification devices. MFA greatly increases the level of difficulty for adversaries to compromise enterprise user accounts, and thus gain access to sensitive customer data."
- "MFA solutions **that protect against credential phishing, such as those using the Web Authentication standard supported by web browsers, are especially important**."
- "If a covered person or service provider does not require MFA for its employees or offer multi-factor authentication as an option for consumers accessing systems and accounts, or has not implemented a reasonably secure equivalent, **it is unlikely that the entity could demonstrate that countervailing benefits to consumers or competition outweigh the potential harms, thus triggering liability.**"

VENABLE LLP

# What's New Here?

- FFIEC guidance on "Authentication and Access to Financial Institution Services and Systems" has historically focused on laying out criteria for FIs to take a risk-based approach to authentication.
- CFPB is getting more prescriptive – signaling that financial institutions that do not require MFA for their employees or offer multi-factor authentication as an option for consumers may face consequences.
- CFPB is also signaling that financial institutions should offer "the right MFA" – noting that some legacy MFA tools will not adequately guard against credential phishing attacks.

VENABLE LLP

# Going Beyond Guidance


- FFIEC regulators have long issued guidance to financial institutions on authentication – but this is the first time we've seen one urge consumers to file complaints if their FI doesn't offer it.

VENABLE LLP

# Multi-Factor Authentication (MFA)

**Per CFPB:**

- "Multi-factor authentication (MFA) is a security enhancement that requires multiple credentials (factors) before an account can be accessed."
- "Factors fall into three categories: something you know, like a password; something you have, like a token; and something you are, like your fingerprint."
- "A common MFA setup is supplying both a password and a temporary numeric code in order to log in. Another MFA factor is the use of hardware identification devices. MFA greatly increases the level of difficulty for adversaries to compromise enterprise user accounts, and thus gain access to sensitive customer data."
- "MFA solutions **that protect against credential phishing, such as those using the Web Authentication standard supported by web browsers, are especially important**."
- "If a covered person or service provider does not require MFA for its employees or offer multi-factor authentication as an option for consumers accessing systems and accounts, or has not implemented a reasonably secure equivalent, **it is unlikely that the entity could demonstrate that countervailing benefits to consumers or competition outweigh the potential harms, thus triggering liability.**"

VENABLE LLP

# MFA & Web Authentication – Why the Callout?

- "Legacy" MFA – tools that require a one-time passcode (OTP) or a response to a push-notification sent to an authentication app – is not as secure as it used to be.
- Attackers have caught up – and can easily phish OTP codes or trick someone into pushing "approve" when they get a prompt on their mobile device to verify a login.
- With push-based apps, "MFA Fatigue" is an attack where an adversary has a stolen password and continues to "bomb" a target's app with login prompts – often accompanied by emails, texts, or phone calls pretending to be the company verifying the login.
- All it takes is one push of the "Approve" button for an adversary to take over an account.

BLEEPINGCOMPUTER

**MFA Fatigue: Hackers' new favorite tactic in high-profile breaches**

By Lawrence Abrams

September 20, 2022 06:30 AM 1

Hackers are more frequently using social engineering attacks to gain access to corporate credentials and breach large networks. One component of these attacks that is becoming more popular with the rise of multi-factor authentication is a technique called MFA Fatigue.

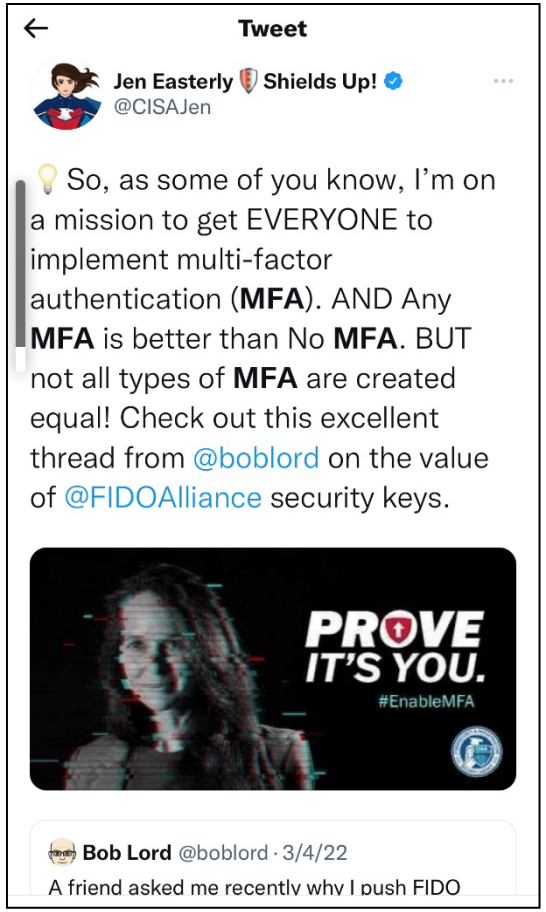
When breaching corporate networks, hackers commonly use stolen employee login credentials to access VPNs and the internal network.

VENABLE LLP

# MFA & Web Authentication – Why the Callout?

- Web Authentication (aka "FIDO Authentication") is a newer authentication standard that guards against these credential phishing attacks
- CISA calls FIDO authentication the "gold standard" of MFA – and has been highlighting that all MFA is not created equal
- Support for FIDO/Web Authentication is built in "out of the box" in major browsers and tech operating systems – meaning the barrier to implementing it both in the enterprise and for consumers is lower than other forms of MFA

**Our take: Attackers have caught up with legacy MFA; FIs can best mitigate this risk by implementing FIDO authentication internally and for consumers.**




VENABLE LLP

# Password Management

Notable snippets from the CFPB Circular

"If a covered person or service provider **does not have adequate password management policies and practices**, it is unlikely they would succeed in showing countervailing benefits to consumers or competition that outweigh the potential harms, **thus triggering liability.**"

"This includes **failing to have processes in place to monitor for breaches at other entities** where employees may be re-using logins and passwords (including notifying users when a password reset is required as a result), and includes **use of default enterprise logins or passwords**."

VENABLE LLP

# Password Management

Why now?

- Password/User Account breaches continue to be one of the primary enablers for further identity theft and cyberattacks. An evolving threat landscape presents new challenges:
  - Ongoing compromise of Password Manager applications (LastPass hack, 2022)
  - Accumulated “bad passwords” from other breaches (~11.9 billion breached accounts)
  - Increased hardware/software capabilities of attacks, making old hashing methods obsolete

# Password Management

Context and background

- The CFPB Circular aligns with previous password guidance as published by NIST in SP 800-63B: Digital Identity Guidelines.
- SP 800-63B, in particular the requirements in Section 5.1.1 and the informative guidance in Appendix A, is widely considered to be best practice.
- However, the text of the CFPB focuses on password breaches and default passwords, only a small part of the NIST guidance.
  - The suggestion to do continuous monitoring of password breaches at other entities goes above 800-63B recommendations.

# Password Management

Dealing with explicitly included issues

- Comparing newly requested passwords against a database of known breached passwords and common or default passwords meets the first portion of the Circular's suggestion.
  - In-depth password databases can be purchased or subscribed to as a service from many security and identity vendors.
  - Some free sources are available, with less guarantee of completeness, such as https://haveibeenpwned.com.
- Ongoing monitoring of breaches at other entities is more difficult to quantify and deal with.
  - Continuous breach monitoring is a service offered by many security and identity vendors.
  - Regularly checking the same lists used at password creation time may qualify as an "adequate process."

# Password Management

Potentially implied further requirements

- The CFPB Circular does not provide an exhaustive list of what qualifies as "adequate password management policies," though it does provide a link to a CISA Good Security Habits page.
- Groups looking to take a more cautious approach may wish to enforce a wider set of password requirements as laid out in NIST SP 800-63B, such as:
  - Using secure cryptographic practices (encryption, salting, and hashing) to protect user passwords in transit and at rest
  - Implementing rate-limiting and server/network cybersecurity
  - Using proven composition and complexity rules
  - Avoiding arbitrary password requirements and password expiration timelines

VENABLE LLP

# Timely Software Updates

Notable snippets from the CFPB Circular

"If covered persons or service providers **do not routinely update systems, software, and code** (including those utilized by contractors) **or fail to update them when notified of a critical vulnerability**, it is unlikely they would succeed in showing countervailing benefits to consumers or competition that outweigh the potential harms, **thus triggering liability.**"

"This includes **not having asset inventories** of which systems contain dependencies on certain software to make sure software is up to date and highlight needs for patches and updates. It also includes **the use of versions of software that are no longer actively maintained by their vendors**."

VENABLE LLP

# Timely Software Updates

Background and context

- The circular makes explicit reference to CFPB's legal complaint against Equifax in 2017, in which Equifax was accused of using antiquated and poorly maintained software that contained known vulnerabilities.
- Given the above complaint reference to Common Vulnerability Enumeration (CVE), "critical vulnerability" likely refers to a given vulnerability's Common Vulnerability Scoring System (CVSS) score as provided by NIST at the National Vulnerability Database (NVD).

# Timely Software Updates

Addressing CFPB concerns

- Perfect asset, vulnerability, and patch management is likely impossible for any moderately large enterprise.
- The CFPB Circular implies a minimum level of due diligence to mitigate the potential for being found liable in the case of a breach:
  - Routinely check for updates for the software and assets that you and your contractors use. This includes applications, operating systems, web browsers, and IoT firmware.
  - Maintain a reliable inventory of the software assets in use at your enterprise, along with their versions.
  - Routinely cross-check your asset inventory against lists of known vulnerabilities, such as the NVD.

# Timely Software Updates

Recent developments

- There has been an increased focus on this issue in the federal government, including the NIST Cyber Security Framework (CSF), the National Telecommunications and Information Administration (NTIA)'s Software Bill of Materials (SBOM) publications, and the inclusion of cyber provisions in the National Defense Authorization Act for FY2022 (NDAA).
- The minimum level of due diligence as described previously is roughly common practice across industry, but it is possible that action from the CFPB or other agencies will hold financial organizations to a higher standard.

# Bank/Fintech Partnerships

- Developments in open banking, banking-as-a-service, and payments change the way consumers and businesses interact with financial services providers.
- Underlying all of these changes is the sharing of customer data between fintechs, traditional financial institutions, and data aggregators.
- Examples of open banking use cases
  - Making and receiving payments
  - Loan underwriting
  - Account ownership validation / identity verification
  - Budgeting / personal financial account management products and services
  - Financial advisory services

VENABLE LLP

# Reasons Why Bank Partnerships Are Used for Many Fintech Products and Services

All fintechs need a bank partner in some way:

- Leveraging of existing bank platforms and services
- Establishing products and services in a way that minimizes licensing requirements for fintechs
  - Money transmission
  - Lending / usury
  - Payment network requirements
- Access to data

VENABLE LLP

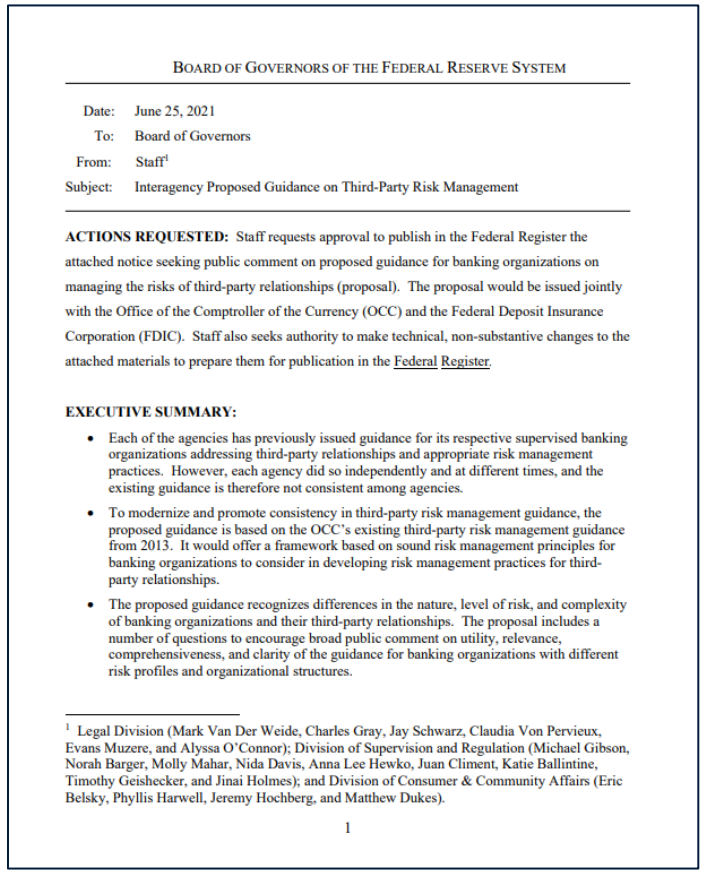
# Increased Regulatory Scrutiny of BaaS: OCC Agreement with Blue Ridge Bank (August 2022)

- Focus on unsafe and unsound practices related to third-party risk management, AML, suspicious activity reporting, and information technology control and risk governance.
- Required bank to create a compliance committee to oversee and report to OCC on compliance with the agreement.
- Specific requirements / areas for improvement included:
  - Implement a written program to manage the risks posed by third-party fintech relationships.
  - Obtain "no objection" confirmation from OCC prior to onboarding new fintechs or expanding current relationships.
    - Improve AML compliance
    - Audits
    - Staffing
    - Customer due diligence
    - Suspicious activity monitoring and reporting (including a look back review)
- Implement written program to manage information technology (IT) activities, including those activities conducted through fintech relationships.

VENABLE LLP

# Importance of Third-Party Risk Management

- The federal bank regulatory agencies have requested public comment on proposed guidance designed to help banking organizations manage risks associated with third-party relationships, including relationships with financial technology-focused entities. The proposed guidance is intended to assist banking organizations in identifying and addressing the risks associated with third-party relationships and responds to industry feedback requesting alignment among the agencies with respect to third-party risk management guidance.
- "Third-party relationships can include relationships with entities such as vendors, financial technology (fintech) companies, affiliates, and the banking organization's holding company."
- July 19, 2021 – NPRM issued
- September 17, 2021 – Public comment period closed



BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

Date: June 25, 2021
To: Board of Governors
From: Staff[1]
Subject: Interagency Proposed Guidance on Third-Party Risk Management

**ACTIONS REQUESTED:** Staff requests approval to publish in the Federal Register the attached notice seeking public comment on proposed guidance for banking organizations on managing the risks of third-party relationships (proposal). The proposal would be issued jointly with the Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC). Staff also seeks authority to make technical, non-substantive changes to the attached materials to prepare them for publication in the Federal Register.

**EXECUTIVE SUMMARY:**

- Each of the agencies has previously issued guidance for its respective supervised banking organizations addressing third-party relationships and appropriate risk management practices. However, each agency did so independently and at different times, and the existing guidance is therefore not consistent among agencies.
- To modernize and promote consistency in third-party risk management guidance, the proposed guidance is based on the OCC's existing third-party risk management guidance from 2013. It would offer a framework based on sound risk management principles for banking organizations to consider in developing risk management practices for third-party relationships.
- The proposed guidance recognizes differences in the nature, level of risk, and complexity of banking organizations and their third-party relationships. The proposal includes a number of questions to encourage broad public comment on utility, relevance, comprehensiveness, and clarity of the guidance for banking organizations with different risk profiles and organizational structures.

[1] Legal Division (Mark Van Der Weide, Charles Gray, Jay Schwarz, Claudia Von Pervieux, Evans Muzere, and Alyssa O'Connor); Division of Supervision and Regulation (Michael Gibson, Norah Barger, Molly Mahar, Nida Davis, Anna Lee Hewko, Juan Climent, Katie Ballintine, Timothy Geishecker, and Jinai Holmes); and Division of Consumer & Community Affairs (Eric Belsky, Phyllis Harwell, Jeremy Hochberg, and Matthew Dukes).

1

VENABLE LLP

# Questions?


**Andrew E. Bigart**
Partner
+ 1 202.344.4323
aebigart@Venable.com

**Jeremy A. Grant**
Managing Director of Technology Business Strategy
+ 1 202.344.4646
jagrant@Venable.com

**Alexandra Megaris**
Partner
+1 212.370.6210
amegaris@Venable.com

**Ross B. Nodurft**
Senior Director of Cybersecurity Services
+1 202.344.4403
rbnodurft@Venable.com


VENABLE LLP

VENABLE LLP