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.

Acts or practices are unfair when they cause or are likely to cause substantial injury that is not reasonably avoidable or outweighed by countervailing benefits to consumers or competition. Inadequate authentication, password management, or software update policies or practices are likely to cause substantial injury to consumers that is not reasonably avoidable by consumers, and financial institutions are unlikely to successfully justify weak data security practices based on countervailing benefits to consumers or competition. Inadequate data security can be an unfair practice in the absence of a breach or intrusion.

Analysis

Widespread data breaches and cyberattacks have resulted in significant harms to consumers, including monetary loss, identity theft, significant time and money spent dealing with the impacts of the breach, and other forms of financial distress. Providers of consumer financial

services are subject to specific requirements to protect consumer data. In 2021, the Federal Trade Commission (FTC) updated its Safeguards Rule implementing Section 501(b) of GLBA, to set forth specific criteria relating to the safeguards that certain nonbank financial institutions must implement as a part of their information security programs.[1] These safeguards, among other things, limit who can access customer information, require the use of encryption to secure such information, and require the designation of a single qualified individual to oversee an institution's information security program and report at least annually to the institution's board of directors or equivalent governing body. The federal banking agencies also have issued interagency guidelines to implement Section 501 of GLBA.[2]

In certain circumstances, failure to comply with these specific requirements may also violate the CFPA's prohibition on unfair acts or practices. The CFPA defines an unfair act or practice as an act or practice: (1) that causes or is likely to cause substantial injury to consumers, (2) which is not reasonably avoidable by consumers, and (3) is not outweighed by countervailing benefits to consumers or competition.[3]

A practice causes substantial injury to consumers when it causes significant harm to a few consumers or a small amount of harm to many consumers. For example, inadequate data security measures can cause significant harm to a few consumers who become victims of targeted identity theft as a result, or it can cause harm to potentially millions of consumers when there are large customer-base-wide data breaches. Information security weaknesses can result in data breaches, cyberattacks, exploits, ransomware attacks, and other exposure of consumer data.[4]

Further, actual injury is not required to satisfy this prong in every case. A significant risk of harm is also sufficient. In other words, this prong of unfairness is met even in the absence of a data breach. Practices that "are likely to cause" substantial injury, including inadequate data

[1] 86 Fed. Reg. 70272 (Dec. 9, 2021).

[2] *See* 66 Fed. Reg. 8616 (Feb. 1, 2001). These guidelines are currently codified at 12 CFR pt. 30, Appendix B (OCC); Regulation H, 12 CFR 208, Appendix D-2 (Board); Regulation Y, 12 CFR 225, Appendix F (Board); 12 CFR pt. 364, Appendix B (FDIC).

[3] 12 U.S.C. § 5531(c). The unfairness standard in the CFPA is similar to the unfairness standard in Section 5 of the Federal Trade Commission Act.

[4] *Compliance Management Review – Information Technology*, CFPB Examination Procedures (Sept. 2021), https://files.consumerfinance.gov/f/documents/cfpb_compliance-management-review-information-technology_examination-procedures.pdf.

security measures that have not yet resulted in a breach, nonetheless satisfy this prong of unfairness.[5]

Consumers cannot reasonably avoid the harms caused by a firm's data security failures. They typically have no way of knowing whether appropriate security measures are properly implemented, irrespective of disclosures provided. They do not control the creation or implementation of an entity's security measures, including an entity's information security program. And consumers lack the practical means to reasonably avoid harms resulting from data security failures.[6]

Where companies forgo reasonable cost-efficient measures to protect consumer data, like those measures identified below, the Consumer Financial Protection Bureau (CFPB) expects the risk of substantial injury to consumers will outweigh any purported countervailing benefits to consumers or competition. The CFPB is unaware of any instance in which a court applying an unfairness standard has found that the substantial injury caused or likely to have been caused by a company's poor data security practices was outweighed by countervailing benefits to consumers or competition.[7] Given the harms to consumers from breaches involving sensitive financial information, this is not surprising.

Relevant Precedent

On July 22, 2019, the CFPB alleged that Equifax violated the CFPA's prohibition on unfair acts or practices.[8] The FTC also alleged that Equifax violated the FTC Act and the FTC's Safeguards Rule, which implements Section 501 of GLBA and establishes certain requirements that nonbank financial institutions must adhere to in order to protect financial information.[9]

---

[5] *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 246 (3d Cir. 2015) ("Although unfairness claims 'usually involve actual and completed harms,' 'they may also be brought on the basis of likely rather than actual injury,' '[and] the FTC Act expressly contemplates the possibility that conduct can be unfair before actual injury occurs.'") (interpreting unfairness standard in the FTC Act, for which precedent is often used in interpreting the similar CFPA standard) (citations omitted).

[6] *FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1115 (S.D. Cal. 2008) ("[C]onsumers who had their bank accounts accessed without authorization had no chance whatsoever to avoid the injury before it occurred.").

[7] *FTC v. Neovi,* 604 F.3d 1150, 1158 (9th Cir. 2010) ("The FTC also met its burden of showing that consumer injury was not outweighed by countervailing benefits to consumers or to competition."); *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014) (defendant challenged first two elements, but not the countervailing benefits finding).

[8] Complaint at 39-53, *BCFP v. Equifax, Inc.*, 1:19-cv-03300 (N.D. Ga. July 22, 2019), https://files.consumerfinance.gov/f/documents/cfpb_equifax-inc_complaint_2019-07.pdf. The FTC also alleged that Equifax violated the FTC Act's prohibition on unfair acts or practices.

[9] Complaint at 45-46, *FTC v. Equifax, Inc.*, 1:19-mi-99999-UNA (N.D. Ga. July 22, 2019), https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_complaint_7-22-19.pdf.

In its complaint against Equifax, the CFPB alleged an unfairness violation based on Equifax's failure to provide reasonable security for sensitive personal information it collected, processed, maintained, or stored within computer networks.[10] In particular, Equifax violated the prohibition on unfairness (as well as the FTC's Safeguards Rule) by using software that contained a known vulnerability and failing to patch the vulnerability for more than four months. Hackers exploited the vulnerability to steal over 140 million names, dates of birth, and SSNs, as well as millions of telephone numbers, email addresses, and physical addresses, and hundreds of thousands of credit card numbers and expiration dates.[11]

Before the Equifax matter, law enforcement actions related to inadequate authentication triggered liability under the FTC Act's prohibition on unfair practices. In 2006, the FTC sued online check processor Qchex and related entities for violating the FTC Act. The FTC alleged that it was an unfair practice to create and deliver checks without verifying that the person requesting the check was authorized to draw checks on the associated bank account.[12] Qchex created checks "even when the customer's name differed from the name on the bank account listed on the checks or from the name on the credit card account the customer used to pay for [Qchex's] services."[13]

Even after setting up certain identity verification procedures, Qchex bypassed those procedures for some customers.[14] Ultimately, a court observed, "it was a simple matter for unscrupulous opportunists to obtain identity information and draw checks from accounts that were not their own."[15] That court confirmed that Qchex injured consumers by creating and delivering unverified checks, in violation of Section 5 of the FTC Act.[16] Implementation of common-sense practices—including those that are now required under the FTC's Safeguards Rule—protects consumers from injury and that, in turn, mitigates potential liability for businesses.

Liability for unfair acts or practices has also been triggered in the context of password management and routine software updates. In 2012, the FTC sued multiple entities associated with the Wyndham hospitality company for their failures "to employ reasonable and appropriate

---

[10] Complaint at 40-42, *BCFP v. Equifax, Inc.*, https://files.consumerfinance.gov/f/documents/cfpb_equifax-inc_complaint_2019-07.pdf.

[11] The CFPB, FTC, and state Attorneys General imposed $700 million in relief and penalties against Equifax.

[12] *See* Complaint at 10, *FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104 (S.D. Cal. 2008) (No. 06 Civ. 1952), *aff'd*, 604 F.3d 1150 (9th Cir. 2010).

[13] *Id.* at 5.

[14] *Id.* at 6.

[15] *Neovi, Inc.*, 604 F.3d at 1154.

[16] *Id.* at 1157.

measures to protect personal information against unauthorized access" in violation of the FTC Act's prohibitions on deceptive and unfair acts and practices.[17] The inadequate data security practices included "using outdated operating systems that could not receive security updates or patches to address known security vulnerabilities," servers that used "well-known default user IDs and passwords…which were easily available to hackers through simple Internet searches," and password management policies that did not require "the use of complex passwords for access to the Wyndham-branded hotels' property management systems and allow[ing] the use of easily guessed passwords."[18]

The FTC alleged that, due to these and other deficient security measures, "intruders were able to gain unauthorized access to [Wyndham's] computer network…on three separate occasions" and retrieved "customers' payment card account numbers, expiration dates, and security codes."[19] One such incident led to "the compromise of more than 500,000 payment card accounts, and the export of hundreds of thousands of consumers' payment card account numbers to a domain registered in Russia."[20] When Wyndham argued that data security issues were outside the bounds of the FTC's unfairness authority, the courts confirmed that "the FTC has authority to regulate cybersecurity under the unfairness prong of" Section 5(a) of the FTC Act and that regulated entities have adequate notice that cybersecurity issues could lead to violations of that provision.[21]

In March 2022, the FTC announced an administrative complaint and proposed consent orders against Residual Pumpkin Entity, LLC and PlanetArt, LLC, respectively the former and current operators of CafePress, a customized merchandise e-commerce platform.[22] The FTC's complaint documented several inadequate data security practices, including the failure to "implement patch management policies and procedures to ensure timely remediation of critical security vulnerabilities," the failure to "establish or enforce rules sufficient to make user credentials (such as username and password) hard to guess," the failure to disclose security incidents to

[17] First Amended Complaint at 19, *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 13 Civ. 1887), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

[18] *Id.* at 11.

[19] *Id.* at 12-13.

[20] *Id.* at 15.

[21] *Wyndham Worldwide Corp.*, 799 F.3d at 240.

[22] CafePress, 87 Fed. Reg. 16187 (FTC Mar. 22, 2022) (analysis of proposed consent orders to aid public comment).

relevant parties, and inadequate "measures to prevent account takeovers through password resets using data known to have been obtained by hackers."[23]

While the prohibition on unfair practices is fact-specific, the experience of the agencies suggests that failure to implement common data security practices will significantly increase the likelihood that a firm may be violating the prohibition. In the examples below, the Circular describes conduct that will typically meet the first two elements of an unfairness claim (likely to cause substantial injury to consumers that is not reasonably avoidable by consumers), and thus increase the likelihood that an entity's conduct triggers liability under the CFPA's prohibition of unfair practices.

1. Multi-factor authentication

Multi-factor authentication (MFA) is a security enhancement that requires multiple credentials (factors) before an account can be accessed.[24] 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.[25]

[23] Complaint at 4-5, *In re Residual Pumpkin Entity, LLC and PlanetArt, LLC*, No. 1923209, (FTC June 23, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/1923209CafePressComplaint.pdf.

[24] *Back to Basics: What's multi-factor authentication - and why should I care?*, National Institute of Standards and Technology, https://www.nist.gov/blogs/cybersecurity-insights/back-basics-whats-multi-factor-authentication-and-why-should-i-care.

[25] For a more thorough discussion of MFA, please refer to Cybersecurity & Infrastructure Security Agency's (CISA's) Multi-Factor Authentication page, or the National Institute of Standards and Technology's (NIST's) Digital Identity Guidelines. *Multi-Factor Authentication*, CISA, https://www.cisa.gov/mfa; *Digital Identity Guidelines: Authentication and Lifecycle Management*; *Authenticator Assurance Level 2*, NIST, (June 2017), https://pages.nist.gov/800-63-3/sp800-63b.html.

2. Password Management

Unauthorized use of passwords is a common data security issue. Username and password combinations can be sold on the dark web or posted for free on the internet, which can be used to access not just the accounts in question, but other accounts held by the consumer or employee.

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. [26] 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.

3. Timely Software Updates

Software vendors regularly update software to address security vulnerabilities within a program or product. When patches are released, the public, including hackers, become aware of the prior vulnerabilities. Therefore, when companies use commonly available software, including open-source software and open-source libraries, [27] and do not install a patch that has been released for that software or take other mitigating steps if patching is not possible, they neglect to fix a security vulnerability that has become widely known. As noted in the CFPB's complaint against Equifax, Equifax's 2017 failure to patch a known vulnerability resulted in hackers gaining access to Equifax's systems that exposed the personal information of nearly 148 million consumers. [28]

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

[26] *Good Security Habits*, CISA, (Feb. 1, 2021), Good Security Habits | CISA.

[27] *FTC warns companies to remediate Log4j security vulnerability* (Jan. 4, 2022), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability. ("Log4j is a ubiquitous piece of software used to record activities in a wide range of systems found in consumer-facing products and services. Recently, a serious vulnerability in the popular Java logging package, Log4j (CVE-2021-44228) was disclosed, posing a severe risk to millions of consumer products to enterprise software and web applications.")

[28] Complaint at 13, *BCFP v. Equifax, Inc.*, https://files.consumerfinance.gov/f/documents/cfpb_equifax-inc_complaint_2019-07.pdf.

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.

About Consumer Financial Protection Circulars

Consumer Financial Protection Circulars are issued to all parties with authority to enforce federal consumer financial law. The Consumer Financial Protection Bureau (CFPB) is the principal federal regulator responsible for administering federal consumer financial law, *see* 12 U.S.C. 5511, including the Consumer Financial Protection Act's prohibition on unfair, deceptive, and abusive acts or practices, 12 U.S.C. 5536(a)(1)(B), and 18 other "enumerated consumer laws," 12 U.S.C. 5481(12). However, these laws are also enforced by state attorneys general and state regulators, 12 U.S.C. 5552, and prudential regulators including the Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the National Credit Union Administration. *See, e.g.*, 12 U.S.C. 5516(d), 5581(c)(2) (exclusive enforcement authority for banks and credit unions with $10 billion or less in assets). Some federal consumer financial laws are also enforceable by other federal agencies, including the Department of Justice and the Federal Trade Commission, the Farm Credit Administration, the Department of Transportation, and the Department of Agriculture. In addition, some of these laws provide for private enforcement.

Consumer Financial Protection Circulars are intended to promote consistency in approach across the various enforcement agencies and parties, pursuant to the CFPB's statutory objective to ensure federal consumer financial law is enforced consistently. 12 U.S.C. 5511(b)(4). *Consumer Financial Protection Circulars* are also intended to provide transparency to partner agencies regarding the CFPB's intended approach when cooperating in enforcement actions. *See, e.g.*, 12 U.S.C. 5552(b) (consultation with CFPB by state attorneys general and regulators); 12 U.S.C. 5562(a) (joint investigatory work between CFPB and other agencies).

Consumer Financial Protection Circulars are general statements of policy under the Administrative Procedure Act. 5 U.S.C. 553(b). They provide background information about applicable law, articulate considerations relevant to the Bureau's exercise of its authorities, and, in the interest of maintaining consistency, advise other parties with authority to enforce federal consumer financial law. They do not restrict the Bureau's exercise of its authorities, impose any legal requirements on external parties, or create or confer any rights on external parties that could be enforceable in any administrative or civil proceeding. The CFPB Director is instructing CFPB 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.