BILLING CODE: 4810-AM-P

CONSUMER FINANCIAL PROTECTION BUREAU

Docket No.: CFPB-2025-0005

Request for Information Regarding the Collection, Use, and Monetization of Consumer Payment and Other Personal Financial Data

AGENCY: Consumer Financial Protection Bureau.

ACTION: Notice and request for information.

SUMMARY: The Consumer Financial Protection Bureau (CFPB) is seeking comments from the public to better understand how companies that offer or provide consumer financial products or services collect, use, share, and protect consumers' personal financial data, such as data harvested from consumer payments. The submissions in response to this request for information will serve to assist the CFPB and policymakers in further understanding the current state of the business practices at these companies and the concerns of consumers as the CFPB exercises its enforcement, supervision, regulatory, and other authorities.

DATES: Comments must be received on or before April 11, 2025.

ADDRESSES: You may submit comments, identified by Docket No. CFPB-2025-0005, by any of the following methods:

- *Federal eRulemaking Portal:* https://www.regulations.gov. Follow the instructions for submitting comments.
- *Email: PrivacyRFI@cfpb.gov.* Include the document title and Docket No. CFPB-2025-0005 in the subject line of the message.
- *Mail/Hand Delivery/Courier:* Comment Intake, Request for Information Regarding Financial Company Consumer Data, Consumer Financial Protection Bureau, c/o Legal Division Docket Manager, 1700 G Street, NW, Washington, DC 20552. Because paper mail in the Washington,

DC area and at the CFPB is subject to delay, commenters are encouraged to submit comments electronically.

Instructions: The CFPB encourages the early submission of comments. All submissions should include the agency name and docket number for this request for information. Please note the number of the topic on which you are commenting at the top of each response (you do not need to address all topics). In general, all comments received will be posted without change to https://www.regulations.gov. All comments, including attachments and other supporting materials, will become part of the public record and subject to public disclosure. Proprietary or sensitive personal information, such as account numbers or Social Security numbers, or the names of other individuals should not be included. Comments will not be edited to remove any identifying or contact information or other information that you would ordinarily not make public.

FOR FURTHER INFORMATION CONTACT: George Karithanom, Regulatory Implementation and Guidance Program Analyst, Office of Regulations, at 202-435-7700 or at: https://reginquiries.consumerfinance.gov/. If you require this document in an alternative electronic format, please contact CFPB_Accessibility@cfpb.gov.

SUPPLEMENTARY INFORMATION:

I. Background

A. Recent CFPB Efforts on Payment Privacy

Over the last decade, Americans have increasingly adopted new ways to make payments, particularly through digital payment services and applications operating adjacent to, but outside of, the traditional banking system. Since 2021, the CFPB has conducted extensive research into the changing landscape of consumer payments, which included information obtained through market monitoring orders issued to large technology companies offering digital payment apps. For example, in 2022, the CFPB published a report about the convergence of payments with other commercial activities in the

United States and abroad.[1] The report noted some of the types of data captured in these "super apps," including apps that are ubiquitous in China. As part of its development of the Personal Financial Data Rights Rule required by section 1033 of the Consumer Financial Protection Act, the CFPB closely studied ways in which financial data can be protected in the context of data portability and "open banking."[2]

Across these efforts, the CFPB has observed that actual business practices show significant deviation from longstanding consumer expectations when it comes to the collection, use, and monetization of data harvested from payment transactions. Americans may think that their financial information is kept private just because it is sensitive. However, the CFPB's monitoring of the market suggests that companies operating payment systems and apps are able to connect payments data with a broad range of other data. The CFPB also notes that there have been significant advances in the capabilities of physical devices and hardware, giving these companies the technical capability to collect biometric information (including certain vital signs and the voices of individuals proximate to the primary user), geographic location, social networking habits, and more. The commingling of this data with personal financial data raises heightened concerns about privacy, given the significant value companies derive from that data. For example, such information could be used to develop dynamic pricing algorithms that tailor prices to a particular individual, where the seller is aided by knowledge about the consumer's purchase history.

B. The Gramm-Leach-Bliley Act and Regulation P

In 1999, Congress enacted the Gramm-Leach-Bliley Act (GLBA),[3] which authorized bank holding companies and financial holding companies to engage, directly and through their affiliates, in

[1] CFPB, *The Convergence of Payments and Commerce* (Aug. 2022), https://files.consumerfinance.gov/f/documents/cfpb_convergence-payments-commerce-implications-consumers_report_2022-08.pdf.
[2] Required Rulemaking on Personal Financial Data Rights, 89 FR 90838 (Nov. 18, 2024).
[3] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999).

a wide variety of "financial activities" that extended far beyond traditional banking.[4] At the same time, Congress sought to protect consumers by imposing restrictions on how financial institutions share the information they receive about consumers with nonaffiliated third parties. These privacy provisions apply to "financial institution[s]," which Congress broadly defined to include most companies in "the business of . . . engaging in financial activities."[5] For example, banks, credit card issuers, credit bureaus, mortgage originators and servicers, student loan servicers, debt collectors, and payday lenders generally qualify as financial institutions subject to the GLBA.

The privacy provisions of the GLBA protect consumers' "nonpublic personal information"—a term that the GLBA defines broadly.[6] The GLBA limits the extent to which financial institutions can disclose nonpublic personal information to nonaffiliated third parties,[7] and also restricts how downstream recipients of such consumer data can use or further disclose that data.[8]

Initially, the GLBA gave rulemaking authority to several agencies, which then issued regulations to implement the GLBA.[9] On a few occasions, Congress amended the GLBA and the agencies updated their regulations in response.[10] With the passage of the Consumer Financial Protection Act (CFPA), Congress amended the GLBA's rulemaking provision, granting rulemaking authority for the privacy provisions of the GLBA to the CFPB.[11] The CFPA also gave the CFPB

---

[4] 12 U.S.C. 1843(k).
[5] 15 U.S.C. 6809(3).
[6] 15 U.S.C. 6802(a)–(b); *see also* 15 U.S.C. 6809(4) (defining "nonpublic personal information"); 12 CFR 1016.3(p)–(q) (defining "nonpublic personal information" and "personally identifiable financial information").
[7] *See* 15 U.S.C. 6802(b), (e); 12 CFR 1016.13–15.
[8] *See* 15 U.S.C. 6802(c); 12 CFR 1016.11.
[9] *See* section 504, Pub. L. No. 106-102, 113 Stat. 1439–40; *e.g.*, 65 FR 35162 (June 1, 2000) (codified at 12 CFR parts 40, 216, 332, 573) (final rule implemented by the Office of the Comptroller of the Currency, the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision); 65 FR 33646 (May 24, 2000) (codified at 12 CFR part 313) (final rule implemented by the Federal Trade Commission).
[10] *E.g.*, section 75001, Pub. L. No. 114-94, 129 Stat. 1312, 1787 (2015); section 728, Pub. L. No. 109-351, 120 Stat. 1966, 2003–04 (2006).
[11] *See* section 1093, Pub. L. No. 111-203, 124 Stat. 1376, 2095 (July 21, 2010). The CFPB does not have rulemaking authority with respect to the GLBA's data security standards. *See* 15 U.S.C. 6804(a). The Securities and Exchange Commission, Commodity Futures Trading Commission, and Federal Trade Commission also have rulemaking authority within their respective jurisdictions. *See id.*

authority to enforce the GLBA's privacy provisions, along with other Federal regulators.[12] Additionally, the CFPB has used its authority to address unfair or deceptive acts or practices related to the handling of consumer data.[13]

In 2011, the CFPB restated the prior agencies' regulations as Regulation P with certain ministerial changes to reflect the CFPB's role under the GLBA.[14] Since then, the CFPB has only modified Regulation P twice. As part of a streamlining initiative to reduce the burden of regulations it inherited from other agencies, the CFPB approved simplifications in the process for providing certain annual privacy notices.[15] Subsequently, in parallel with other agencies, the CFPB implemented congressional amendments to the GLBA that adjusted the annual notice requirement where certain conditions are met.[16] In most other respects, Regulation P continues to align with the regulations the predecessor agencies first issued to implement the GLBA following its enactment. For example, the CFPB has not revised the model form the predecessor agencies developed in 2009.[17] Given recent changes in the consumer data landscape, the CFPB has determined that it is appropriate to gather available evidence to inform how the CFPB uses its authorities to address privacy concerns with respect to companies that offer or provide consumer financial products or services, including (if warranted) any potential updates to Regulation P. The CFPB has previously sought information from the public on the consumer data practices of data brokers,[18] and in December 2024 published a proposed rule under the Fair Credit Reporting Act that would subject many data brokers that sell

---

[12] *See* 15 U.S.C. 6805.
[13] *See, e.g.*, Consumer Financial Protection Circular 2022-04, *Insufficient data protection or security for sensitive consumer information*, https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/; Compl., *Bureau of Consumer Fin. Prot. v. Equifax Inc.*, No. 1:19-cv-03300-TWT (N.D. Ga. July 22, 2019), https://files.consumerfinance.gov/f/documents/cfpb_equifax-inc_complaint_2019-07.pdf.
[14] 12 CFR pt. 1016; 76 FR 79025 (Dec. 21, 2011).
[15] 79 FR 64057 (Oct. 28, 2014).
[16] 83 FR 40945 (Aug. 17, 2018).
[17] Model Privacy Form, appendix to part 1016, 12 CFR pt. 1016; *Final Model Privacy Form Under the Gramm-Leach-Bliley Act*, 74 FR 62890 (Dec. 1, 2009).
[18] *Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information*, 88 FR 16951 (Mar. 21, 2023).

consumers' sensitive personal and financial information to the statute.[19] This request for information is another step in a series of efforts to examine data collection, use, and monetization, and to gather information from the public to determine whether additional actions are warranted to protect consumer privacy.

A study by the Government Accountability Office (GAO) also identified consumers' concerns over the privacy of their data, and the potential need for a reassessment of Regulation P and its model form.[20] The GAO observed that "[f]inancial institutions collect extensive amounts of personal information about consumers," including but not limited to "the consumer's Social Security number, annual income, . . . outstanding debt, . . . account balance, payment history, and credit card transactions."[21] Notably, according to the GAO, financial institutions may also collect a consumer's social media activity and browsing activity "to compile a customer profile that can later be used for marketing purposes."[22] Although there has been an "increase in awareness and concern among consumers about their privacy," "the consumer opt-out rate is generally low."[23] In particular, the GAO indicated that "[c]onsumers may be largely unaware of how fintech apps use their personal information and the privacy risks that such usage poses."[24] Although "the model privacy form is voluntary," the GAO noted that "it has been widely adopted within the industry."[25] The GAO stated that "the model form provides consumers with limited insight into the specific information that [financial institutions] collect and with whom they share it."[26] The GAO indicated that "the continued proliferation of consumer data sharing suggests the form may be out of date and may not accurately

[19] *Protecting Americans From Harmful Data Broker Practices (Regulation V)*, 89 FR 101402 (Dec. 13, 2024).
[20] U.S. Gov't Accountability Office, *Consumer Privacy: Better Disclosures Needed on Information Sharing by Banks and Credit Unions* (Oct. 2020), https://www.gao.gov/assets/d2136.pdf.
[21] *Id.* at 1, 5.
[22] *Id.* at 11, 13.
[23] *Id.* at 25, 29.
[24] *Id.* at 18.
[25] *Id.* at 23.
[26] *Id.* at 21.

represent the increased and varied ways financial institutions share information compared to when the form was implemented over 10 years ago."[27] The GAO ultimately concluded its report with a recommendation that the CFPB consider updating the model privacy forms.[28] This Request for Information is issued, in part, in response to that GAO recommendation.

II. Overview

A. General Expectations from Consumers Regarding Privacy and Data Protection

Consumers place a high value on their financial data and are particularly concerned about maintaining the privacy of that data.[29] For example, in a 2021 survey, 89 percent of respondents expressed the belief that it should be illegal "for [their] current bank or credit union to give other companies access to personal data about [them] unless [consumers tell the bank to provide it]," and 94 percent of respondents stated that they would not like their "current bank or credit union to give other companies access to personal data" so those other companies could "market products and services to [those consumers]."[30] Similarly, a 2016 survey suggested that Americans are more concerned about the security of their financial data than even their medical records.[31]

At the same time, consumers are also increasingly gravitating toward the use of digital tools across their financial lives, from accessing banking services via mobile apps to making payments

---

[27] *Id.* at 23.
[28] *Id.* at 37.
[29] *See, e.g.*, Consumer Reports, *American Experiences Survey*, *December 2023 Omnibus Results*, at 18–19 (Jan. 2024), https://article.images.consumerreports.org/image/upload/v1704482298/prod/content/dam/surveys/Consumer_Reports_AES_December-2023.pdf (more than 75 percent of respondents said it was "very important" to them that they know "exactly which companies can access [their] banking data" and that their permission be required before banking data can be shared with another company; while 69 percent felt it was "very important" to "limit[] the purposes for which banks can share [their] banking data, for example, for financial services but not for advertising").
[30] Dan Murphy *et al*., *Financial Data: The Consumer Perspective*, at 10 (June 30, 2021), https://finhealthnetwork.org/wp-content/uploads/2021/04/Consumer-Data-Rights-Report_FINAL.pdf.
[31] Centrify, Consumer Trust Survey, *The Corporate Cost of Compromised Credentials* (2016), https://web.archive.org/web/20170430003505/https:/www.centrify.com/resources/centrify-2016-thought-leadership-survey/ (while 78 percent of Americans ranked "credit card or bank statements" as their top fear of being compromised by hacking or a data breach, only 46 percent ranked "health and medical records" so highly).

through products offered by tech companies.[32] Mobile banking became much more widely adopted as a result of the pandemic, reaching 95percent of consumers age 18-25, 90 percent of consumers under 40, 85 percent of consumers in their 40s, and 60 percent of consumers age 56-75.[33] Similarly, the Federal Reserve Bank of Atlanta found that, in 2023, 70 percent of consumers had made at least one payment via mobile phone or tablet, and 72 percent had adopted online or mobile payment services such as PayPal, Venmo, or Cash App.[34] Another survey found that more than two-thirds of consumers have linked a financial application to their checking account.[35]

A variety of stakeholders, including consumer advocates and Members of Congress, have raised concerns about how information collected by companies that offer or provide consumer financial products or services is used. These companies are increasingly sharing purportedly deidentified individual information with advertisers, and seeking to hire from companies experienced in leveraging data.[36]

It is not clear if consumers realize how many financial companies are currently undertaking these practices. Consumers may not be aware of all the ways that financial companies are collecting their data, or that it can be sold. For example, just 20 percent of respondents to a 2021 survey reported being aware that fintech apps use third-party providers to gather consumers' financial data, and only 24 percent knew that fintech apps could sell consumers' personal financial data.[37]

---

[32] *See, e.g.*, *id.* at 12; Ron Shevlin, *Mobile Banking Adoption in the United States Has Skyrocketed (But So Have Fraud Concerns)*, FORBES (July 29, 2021), https://www.forbes.com/sites/ronshevlin/2021/07/29/mobile-banking-adoption-has-skyrocketed-but-so-have-fraud-concerns-what-can-banks-do/.
[33] Shevlin, *supra*.
[34] Fed. Res. Bank of Atlanta, Research Data Report, *2023 Survey and Diary of Consumer Payment Choice*, at 4, 7, 16 (June 3, 2024), https://www.atlantafed.org/-/media/documents/banking/consumer-payments/survey-diary-consumer-payment-choice/2023/sdcpc_2023_report.pdf.
[35] Murphy, *supra* at 12.
[36] *See, e.g.*, Iain Withers & Lawrence White, *Dollars in the detail; banks pan for gold in 'data lakes'*, Reuters (June 21, 2019), https://www.reuters.com/article/us-banks-data/dollars-in-the-detail-banks-pan-for-gold-in-data-lakes-idUSKCN1TM0JG/.
[37] Clearinghouse, *2021 Consumer Survey: Data Privacy and Financial App Usage*, at 6 (Dec. 2021), https://www.theclearinghouse.org/-/media/New/TCH/Documents/Data-Privacy/2021-TCH-ConsumerSurveyReport_Final.

B. *Observations from the CFPB's Inquiry into Payment Platforms Operated by Big Tech and Other Large Technology Firms*

The CFPB launched an inquiry into payment platforms, issuing orders in 2021 and 2023 that sought to collect information on the business practices of six technology firms that offer consumer payment products. These orders were issued to two financial technology firms (Block and PayPal), and four large technology "Big Tech" firms whose initial product offerings did not involve payments, but eventually entered the payments market (Alphabet, Amazon, Apple, and Meta). The CFPB's questions related to the firms' respective payment products, and included requests for basic information about each data field[38] each firm collected and maintained as a result of consumers' use of these products, and how the data is used.

Preliminary findings from these inquiries identified potential risks to consumers. First, these firms collect an immense amount of data through their payment products, including data that goes far beyond what is necessary to facilitate a transaction. Specifically, it is common for these payment products to collect and maintain over one thousand data fields, and one of the products collects tens of thousands of data fields. This data and the predictions derived from it can be quite invasive. For example, the companies' data fields include items that appear to:

(1) Predict a consumer's income, wealth, and propensity to spend money or engage in a transaction;

(2) Estimate a consumer's likelihood of contacting customer service, and apparently use that prediction to prioritize access to a live customer service agent;

(3) "Fingerprint" a consumer's device (e.g., using details like phone carrier and model number to identify a specific phone) and what the consumer does on their device (e.g.,

[38] A data field or data element, at a high level, is the name of the data type being collected, similar to the name of a column in a spreadsheet. More formally, a data field or data element can be defined as, "[a] basic unit of information that has a unique meaning and subcategories (data items) of distinct value. Examples of data elements include gender, race, and geographic location." *Data Element*, NIST Computer Security Resource Center (last visited Jan. 7, 2025), https://csrc.nist.gov/glossary/term/data_element.

identifying the name of a consumer's primary social media platform and screen recording a consumer's interaction on the company's app or website);

(4) Use access to a consumer's contacts to collect not just the name and phone number or email address of each contact, but also potentially capture all details contained in the contact such as their birthday, and even the exchangeable image file format, or EXIF, metadata associated with a contact's picture thumbnail, which can include geolocation data; and

(5) Collect not just the vendor and transaction amount, but the stock keeping unit, or SKU, of what was purchased—*i.e.*, the actual item purchased.

Regardless of the stated purpose for such immense data collection, the firms' access to this data may lead them to use this information for other purposes in the future as the incentives or opportunities to monetize it evolve.

Even to the extent that privacy policies make commitments about data collection and use, the policies may still present challenges for consumers. First, many companies frequently update their privacy policies, and consumers may find it burdensome to stay abreast of and understand the implications of such changes. Second, consumers may have grown reliant on or feel "locked into" a product or service. Such consumers may therefore feel compelled to accept changes that they would not have agreed to when they initially began using the product or service. Third, some companies cross-reference "general" and other privacy policies within their product-specific policies, requiring consumers to stitch together a network of documents that makes it more difficult for consumers to form a complete understanding of how their data is being collected and used.

Finally, several of the firms' data governance practices appear to be so deficient that they were unable or unwilling to provide basic information about much of the sensitive consumer data they collect and maintain, such as the name of the data fields and a description of what data they capture.

These companies, for example, generally lack systemic documentation of the immense consumer data they collect and maintain, and how they use this data. These data governance deficiencies raise substantial questions regarding the firms' ability to meaningfully protect consumers' sensitive data.

C. Critiques of Regulation P

Meanwhile, scholars and others have noted that Regulation P has limits. Since Regulation P envisions that financial institutions might combine required disclosures with other information, there may be an "incentive for sellers to bury the disclosures in other consumer correspondence,"[39] even though the regulation requires privacy notices to be clear and conspicuous.[40] Research suggests consumers often do not understand how companies will use their behavioral or transactional data, even when consumers have purportedly consented to such use.[41] Some scholars propose placing affirmative duties on the companies that consumers trust with their data.[42] Others even propose moving away from the "notice and choice" approach of the GLBA altogether.[43]

While observers have documented the increasing role of financial companies in amassing, processing, and selling consumer data, there is still relatively limited public understanding of the data-related operations of companies that offer or provide consumer financial products and services, and the costs and benefits and larger societal impact of those operations. Further, additional, more recent, or broader studies, surveys, and research beyond those summarized above could help to ensure the

[39] *E.g.*, Kent H. Barnett, *Some Kind of Hearing Officer*, 94 Wash. L. Rev. 515, 570 n.237 (2019) (citing 12 CFR 1016.3(b)(2)(ii)(E)).
[40] *See* 12 CFR 1016.4(a), 1016.5(a)(1), 1016.8(a)(1).
[41] *See* Ramy El-Dardiry *et al.*, *Brave New Data: Policy Pathways for the Data Economy in an Imperfect World*, CPB Netherlands Bureau for Econ. Policy Analysis, at 10 (July 2021), https://www.cpb.nl/sites/default/files/omnidownload/CPB-uk-Policy-Brief-Brave-new-data.pdf ("Consumers cannot see what companies are doing with their data, nor can they read all of the data terms of use or oversee the consequences.").
[42] *E.g.*, Bryce Clayton Newell *et al.*, *Regulating the Data Market: The Material Scope of American Consumer Data Privacy Law*, 45 U. Pa. J. Int'l L. 1055, 1140 & n.493 (2024) (collecting publications discussing possible fiduciary duties); Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 Wash. Univ. L. Rev. 961 (2021) (describing a potential duty of loyalty).
[43] *E.g.*, John A. Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else)*, 66 Cleveland State L. Rev. 559 (2018); Daniel J. Solove & Woodrow Hartzog, *Kafka in the Age of AI and the Futility of Privacy as Control*, 104 Boston Univ. L. Rev. 1021 (2024).

CFPB is fully informed about companies' current practices and consumers' preferences as the CFPB exercises its authorities.

III. Request for Information

This request for information seeks comments from the public on how companies that offer or provide consumer financial products or services collect, use, process, transmit, share, store, aggregate, sell, or otherwise generate insights from or act upon consumer data, as well as potential proposals to revise or reform Regulation P. The CFPB is particularly interested in hearing from individuals, social services organizations, consumer rights and advocacy organizations, legal aid attorneys, academics and researchers, small businesses, financial institutions, and State and local government officials.

The CFPB welcomes stakeholders to submit data and information about the ways companies that offer or provide consumer financial products or services collect, use, and share consumer data, including those companies subject to the GLBA and Regulation P. To assist commenters in developing responses, the CFPB has crafted the below questions that commenters may answer. However, the CFPB is interested in receiving any comments relating to the consumer data that financial companies collect.

Public inquiries

1. Are there studies, surveys, research, or other evidence about the incentives for companies to collect more data than is necessary to provide the consumer financial product or service, including to complete a transaction or payment?
2. Are there studies, surveys, research, or other evidence about the effectiveness of Regulation P?
3. Are there studies, surveys, research, or other evidence about the effectiveness of the privacy policy notices and opt-out notices that financial companies provide consumers?

a. How effective is the Regulation P model form[44] in informing consumers about privacy policies, and enabling easy comparisons among different financial institutions? Are there any shortcomings of the model form in this regard?

b. How effective are the Regulation P opt-out notices[45] in describing how consumers can limit the sharing of their information, and explaining how consumers can exercise any opt-out rights they have at a particular company?

c. Considering the privacy and opt-out notices required under Regulation P, how could companies more clearly explain what information they share with whom, and the choices consumers have to limit that sharing?

d. What tools do regulators need or what actions can regulators take to ensure that financial companies are transparent in how they process, protect, and disclose data about consumers?

e. How prevalent are retroactive changes to privacy policies that implicate previously collected data, *i.e.*, changes that purport to apply to previously collected data?

f. How could companies more clearly explain changes in the scope of the data they collect, how it will be used, and what (if any) limitations are placed on future use of that data?

4. Would it be beneficial to separate the privacy notice required by Regulation P from the opt-out notice required by Regulation P?

5. With respect to providing consumers the opportunity to limit sharing, what proportion of consumers in fact opt out?

    a. What statistical analyses, surveys, studies, or other reports have sought to quantify

[44] *See* Model Privacy Form, appendix to part 1016, 12 CFR pt. 1016.
[45] *See* 12 CFR 1016.7.

the proportion of consumers who opt out?

b. What analyses, surveys, studies, or other reports have examined why consumers opt out?

c. What studies, research, or other sources of recommendations have proposed ways to make the opt-out process easier to use?

6. Are there circumstances in which companies share nonpublic personal information with nonaffiliated third parties before consumers have a reasonable opportunity to opt out of the disclosure?

7. What restrictions, conditions, obstacles, website/app designs, or dark patterns do companies place in the way of consumers who wish to opt out of information sharing?

   a. Are there acts or practices that unreasonably impede consumers from exercising the opt-out right the GLBA and Regulation P provide?

   b. What barriers, if any, impede consumers who wish to opt out from directing a company not to disclose the consumers' nonpublic personal information?

   c. If a company is unable to determine how it uses or shares data, how would the company be able to accurately describe the categories of consumer data it shares with which categories of nonaffiliated third parties in an opt-out disclosure?

8. What are the current shortcomings, if any, of Regulation P in protecting consumers' personally identifiable financial information?

9. What questions do financial companies' data collection and use practices raise regarding compliance with the prohibition against unfair, deceptive, and abusive[46] acts and practices

[46] An abusive act or practice: (1) materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service; or (2) takes unreasonable advantage of:

- a lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service;

under the Consumer Financial Protection Act?

10. Are any revisions to Regulation P warranted to address the exceptions financial institutions use to share nonpublic personal information with nonaffiliated third parties?[47] Would any of the exceptions benefit from clarification or adjustment?
11. What are the opportunities:
    a. To strengthen protections for consumers regarding data about them, including to give consumers more choice about what data is collected and how it is used?
    b. To protect data subject to secondary use, such as to ensure that secondary uses comply with the direction given by the consumer?
    c. To track, control, and protect data in the hands of downstream recipients, such as to require downstream recipients to disclose the use, sale, or sharing of consumer nonpublic personal information to the consumers whose data they possess?
    d. To address the aggregation of data that includes data about consumers that originated with financial companies or was collected digitally, to ensure that the data consumers entrusted to companies that offer or provide consumer financial products or services remains protected even in large databases?
    e. To improve the opt-out process under the GLBA and Regulation P?
    f. To ensure that consumers and financial data enjoy consistent protections, whether they use financial or payment products produced by big tech firms

- the inability of the consumer to protect the interests of the consumer in selecting or using a consumer financial product or service; or
- the reasonable reliance by the consumer on a covered person to act in the interests of the consumer.

12 U.S.C. 5531(d).

[47] *See* 12 CFR 1016.13–15

or traditional consumer finance firms?

g. To ensure that all companies are "playing by the same rules" with respect to consumer data when engaging in the same markets?

12. What types of information should the CFPB regularly collect and publish about how financial companies, especially big tech firms, treat data in payment and financial products? Should the CFPB publish more information about the activities of the nonaffiliated third parties that are part of this ecosystem?
13. Are there studies, surveys, research, or other evidence about how the previous collection of consumer data by financial companies, especially large financial institutions and big tech firms, presents a barrier to entry against others wishing to offer competing consumer financial products or services?
14. What harms, if any, result from current business practices that leverage consumer data originating with financial companies or collected digitally through a financial company? What benefits, if any, do consumers currently enjoy because companies share consumers' nonpublic personal information?
15. What additional tools should regulators use to support potential whistleblowers to report corporate conduct that violates consumers' data protection rights?

Rohit Chopra,

Director, Consumer Financial Protection Bureau.