United States Government Accountability Office

Report to the Chairman, Committee on Banking, Housing, and Urban Affairs, U.S. Senate

October 2020

CONSUMER PRIVACY

Better Disclosures Needed on Information Sharing by Banks and Credit Unions

GAO-21-36

GAO Highlights

Highlights of GAO-21-36, a report to the Chairman, Committee on Banking, Housing, and Urban Affairs, U.S. Senate

October 2020

CONSUMER PRIVACY

Better Disclosures Needed on Information Sharing by Banks and Credit Unions

Why GAO Did This Study

Banks and credit unions maintain a large amount of personal information about consumers. Federal law requires that they have processes to protect this information, including data shared with certain third parties. GAO was asked to review how banks and credit unions collect, use, and share such information and federal oversight of these activities. This report examines, among other things, (1) what personal information banks and credit unions collect, and how they use and share the information; (2) the extent to which they make consumers aware of the personal information they collect and share; and (3) how regulatory agencies oversee such collection, use, and sharing.

GAO reviewed privacy notices from a nongeneralizable sample of 60 banks and credit unions with a mix of institutions with asset sizes above and below $10 billion. GAO also reviewed federal privacy laws and regulations, regulators' examinations in 2014–2018 (the last 5 years available), procedures for assessing compliance with federal privacy requirements, and data on violations. GAO interviewed officials from banks, industry and consumer groups, academia, and federal regulators.

What GAO Recommends

GAO recommends that CFPB update the model privacy form and consider including more information about third-party sharing. CFPB did not agree or disagree with the recommendation but said they would consider it, noting that it would require a joint rulemaking with other agencies.

View GAO-21-36. For more information, contact Alicia Puente Cackley at (202) 512-8678 or CackleyA@gao.gov or Nick Marinos at (202) 512-9342 or MarinosN@gao.gov.

What GAO Found

Banks and credit unions collect, use, and share consumers' personal information—such as income level and credit card transactions—to conduct everyday business and market products and services. They share this information with a variety of third parties, such as service providers and retailers.

The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to provide consumers with a privacy notice describing their information-sharing practices. Many banks and credit unions elect to use a model form—issued by regulators in 2009—which provides a safe harbor for complying with the law (see figure). GAO found the form gives a limited view of what information is collected and with whom it is shared. Consumer and privacy groups GAO interviewed cited similar limitations. The model form was issued over 10 years ago. The proliferation of data-sharing since then suggests a reassessment of the form is warranted. Federal guidance states that notices about information collection and usage are central to providing privacy protections and transparency. Since Congress transferred authority to the Consumer Financial Protection Bureau (CFPB) for implementing GLBA privacy provisions, the agency has not reassessed if the form meets consumer expectations for disclosures of information-sharing. CFPB officials said they had not considered a reevaluation because they had not heard concerns from industry or consumer groups about privacy notices. Improvements to the model form could help ensure that consumers are better informed about all the ways banks and credit unions collect and share personal information.

Excerpts of the Gramm-Leach-Bliley Act Model Privacy Form Showing Reasons Institutions Share Personal Information

Reasons we can share your personal information	Does [name of financial institution] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

Source: Gramm-Leach-Bliley Act Model Privacy Form. | GAO-21-36

Federal regulators examine institutions for compliance with GLBA privacy requirements, but did not do so routinely in 2014–2018 because they found most institutions did not have an elevated privacy risk. Before examinations, regulators assess noncompliance risks in areas such as relationships with third parties and sharing practices to help determine if compliance with privacy requirements needs to be examined. The violations of privacy provisions that the examinations identified were mostly minor, such as technical errors, and regulators reported relatively few consumer complaints.

Contents

Tables

Figures

Abbreviations

CFPB	Consumer Financial Protection Bureau
FCRA	Fair Credit Reporting Act
FDIC	Federal Deposit Insurance Corporation
Federal Reserve	Board of Governors of the Federal Reserve System
fintech apps	financial technology applications
GLBA	Gramm-Leach-Bliley Act
NCUA	National Credit Union Administration
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

October 22, 2020

The Honorable Mike Crapo
Chairman
Committee on Banking, Housing, and Urban Affairs
United States Senate

Dear Mr. Chairman:

The growing collection and use of consumers' personal information by commercial entities have raised concerns about protecting consumer privacy, which have been intensified by large-scale data breaches and the growing use of the internet, social media, and mobile applications. For example, an incident in 2019 compromised the personal information of approximately 100 million individuals who were Capital One credit card customers or were applying for a Capital One credit card.[1] Social media and online applications also make it easier to gather personal information, track online behavior, and monitor individuals' locations and activities.

Policymakers have raised questions about how financial institutions collect, use, and protect sensitive consumer information, and the privacy risks related to the proliferation of this information. Financial institutions collect extensive amounts of personal information about consumers—such as Social Security numbers, credit card transactions, and annual income—in providing financial products and services.

While there is no overarching consumer privacy law in the United States, financial institutions are subject to industry-specific privacy laws.[2] The Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA) restrict how financial institutions can use or share personal

[1]On August 6, 2020, the Office of the Comptroller of the Currency (OCC) assessed an $80 million civil money penalty against Capital One, N.A. and Capital One Bank (USA), N.A. after determining that the bank failed to establish an effective risk-assessment process prior to migrating information technology operations to an internet-based ("cloud") environment.

[2]This report focuses on the use and sharing of personal information by financial institutions in the private sector; therefore, we only describe laws governing these entities. Other laws, primarily the Privacy Act of 1974, govern the collection and use of personal information by government agencies. *See* Pub. L. No. 93-579, 88 Stat. 1896, codified at 5 U.S.C. § 552a.

information about consumers.[3] The Consumer Financial Protection Bureau (CFPB), Federal Deposit Insurance Corporation (FDIC), Board of Governors of the Federal Reserve System (Federal Reserve), Office of the Comptroller of the Currency (OCC), and National Credit Union Administration (NCUA) are among the agencies that regulate and examine the use and sharing of consumer information under these laws.

You asked us to examine the types of personal information that financial institutions collect, use, and share; how they make consumers aware of their information-sharing practices; and federal regulatory oversight of these activities. This report examines (1) what personal information federally regulated banks and credit unions collect about consumers, how they use and share this information, and how consumers may share these data with financial technology applications; (2) the extent to which federally regulated banks and credit unions make consumers aware of the personal information they collect and share; and (3) how federal financial regulatory agencies oversee collection, use, and sharing of consumer personal information by banks and credit unions.[4]

For the first objective, we reviewed consumer application forms for different financial products and interviewed officials from a nongeneralizable sample of 10 banks with more than $10 billion in total assets about their collection, use, and sharing of personal information, and processes for protecting those data. We initially judgmentally selected four large institutions and randomly selected a sample of 11 institutions from CFPB's list of supervised depository institutions with more than $10 billion in total assets, but nine of the randomly selected institutions were not able or willing to be interviewed during the early phases of the Coronavirus Disease 2019 pandemic. Consequently, we judgmentally selected four replacement institutions to interview, with an emphasis on the larger institutions that were more likely to have officials available to meet with us following the onset of the pandemic. We also

[3]Gramm-Leach-Bliley Act, Pub. L. No. 106-102, tit. V, subtit. A, 113 Stat. 1338, 1436-1445 (1999) (codified as amended at 15 U.S.C. §§ 6801-6809); Fair Credit Reporting Act, Pub. L. No. 91-508, tit. VI, 84 Stat. 1114, 1127-1136 (1970) (codified as amended at 15 U.S.C. §§ 1681-1681x).

[4]This report only includes banks and credit unions that are regulated by the CFPB, FDIC, the Federal Reserve, OCC, and NCUA, and does not include the review of other financial institutions, such as nonbank lenders.

reviewed a consumer study related to the use of financial technology applications.[5]

Furthermore, we interviewed representatives of six industry groups and four consumer or privacy groups to obtain their perspectives on bank and credit union privacy practices and any other consumer privacy issues. We used a list of groups that submitted comments to a March 2019 information request from the Senate Committee on Banking, Housing, and Urban Affairs on the collection, use, and protection of sensitive consumer information to identify industry groups representing banks and credit unions and consumer groups that had a range of views about the privacy of consumer information. Two of the groups representing consumer and privacy issues were recommended by another consumer group.

The industry groups were the Independent Community Bankers Association, American Bankers Association, Bank Policy Institute, Consumer Bankers Association, National Association of Federal Credit Unions, and Credit Union National Association. The consumer and privacy groups were the U.S. Public Interest Research Group, World Privacy Forum, Consumer Reports, and National Consumer Law Center. We also asked the 10 banks how financial technology has affected consumer privacy and reviewed statements by banks, financial technology firms, and other stakeholders submitted to the CFPB for its February 2020 Consumer Access to Records symposium.[6]

For the second objective, we collected and reviewed publicly available privacy notices for 60 banks and credit unions that used the model form in GLBA's implementing regulations.[7] Specifically, we selected a nongeneralizable sample of 29 banks and credit unions with total assets of more than $10 billion from a list of such institutions provided to us by CFPB. We also selected a nongeneralizable sample of 31 banks and credit unions with total assets of $10 billion or less. Using data from FDIC and NCUA Reports of Condition and Income (call reports), we selected

[5]The Clearing House, *Consumer Survey: Financial Apps and Data Privacy* (November 2019).

[6]Consumer Financial Protection Bureau, "Consumer Access to Financial Records" (Washington, D.C.: Feb. 26, 2020), accessed March 30, 2020, https://www.consumerfinance.gov/about-us/events/archive-past-events/cfpb-symposium-consumer-access-financial-records/.

[7]*See* 12 C.F.R. pt. 1016, app. We initially selected 62 privacy notices, but discarded two that did not use the model privacy form.

our sample to include institutions supervised by each of the four prudential regulators (FDIC, the Federal Reserve, OCC, and NCUA). We also reviewed guidance on privacy protection principles from the National Institute of Standards and Technology (NIST). In addition, we reviewed reports used in the development of the model privacy form under GLBA, including about consumer testing. We also reviewed a study that analyzed privacy disclosure notices and evaluated the extent to which banks and credit unions use the GLBA model privacy form and interviewed one of the authors.[8] We also interviewed officials from the same 10 banks discussed earlier on how they notify consumers of the banks' disclosure practices and process requests to opt out of (or prevent) such disclosures.

For the third objective, we reviewed federal laws and regulations related to consumer financial privacy. We also reviewed examination materials for CFPB and the four prudential regulators and identified how these agencies set the scope of their risk-based examinations with respect to financial privacy. We also interviewed agency officials, as well as staff who examine financial institutions for compliance with privacy requirements under GLBA, FCRA, and related regulations.

We also reviewed data on violations of privacy requirements under GLBA, FCRA, and related regulations from the five most recent years available during our review (2014–2018) and selected and reviewed results from a nongeneralizable sample of 23 completed examinations (from CFPB and four prudential regulators) that included violations of these requirements. Our selection was based on obtaining a mix of violations from the different regulators. We assessed the reliability of the violations data by interviewing federal regulators about the databases they use to track examination violations and reviewing documentation about the systems used to obtain the data. We found the data to be reliable for purposes of this reporting objective. Lastly, we reviewed regulators' guidance for managing third-party risk and interviewed officials at the four prudential regulators about how their examinations address the risk of noncompliance by third parties with whom banks and credit unions share consumer personal information.

We conducted this performance audit from May 2019 to October 2020 in accordance with generally accepted government auditing standards.

[8]Lorrie Faith Cranor, Pedro Giovanni Leon, and Blase Ur, *A Large-Scale Evaluation of U.S. Financial Institutions' Standardized Privacy Notices* (Pittsburgh, Penn.: Carnegie Mellon University, 2016).

Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Federal Consumer Privacy Laws Governing Financial Institutions

The primary federal laws governing the use and sharing of personal information by financial institutions are the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA), as implemented under federal regulations.[9]

Gramm-Leach-Bliley Act Requirements

Enacted in 1999, GLBA governs the disclosure of nonpublic personal information that a financial institution maintains in connection with providing financial products and services to consumers.[10] Nonpublic personal information can include information provided by a consumer when applying for credit, such as the consumer's Social Security number, annual income, or outstanding debt, or which a financial institution otherwise collects or maintains in connection with providing a financial product or service to a consumer, such as the consumer's account balance, payment history, and credit card transactions.[11]

Specifically, GLBA prohibits a financial institution from disclosing a consumer's nonpublic personal information to nonaffiliated third parties—that is, companies that are not related to the financial institution by common ownership or control—unless the institution first has provided the consumer with notice and an opportunity to opt out of (or prevent) the disclosure.[12] There are a number of exceptions to this requirement. For

[9]In addition to federal laws, financial institutions also may be subject to state or international laws that regulate the collection, use, or disclosure of consumer personal information. *See, e.g.*, California Consumer Protection Act, Cal. Civ. Code §§ 1798.100-1798.199, and the European Union's General Data Protection Regulation, Regulation 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119) 1.

[10]Under GLBA, a consumer is an individual who obtains, from a financial institution, financial products or services primarily for personal, family, or household purposes, and the legal representative of such an individual. 15 U.S.C. § 6809(9). *See also* 12 C.F.R. § 1016.3(e).

[11]15 U.S.C. § 6809(4); 12 C.F.R. § 1016.3(p)-(r).

[12]Disclosure is not permitted if the consumer opts out. 15 U.S.C. § 6802; 12 C.F.R. § 1016.10.

example, financial institutions are not required to offer consumers an opportunity to opt out of disclosures to the institution's service providers, such as companies that market the financial institution's products and services, support mobile banking, print checks, and issue credit and debit cards.[13] Other exceptions to the opt-out requirement include disclosures to consumer reporting agencies in accordance with FCRA, and disclosures to comply with civil, criminal, and regulatory investigations.[14]

In addition, GLBA restricts how third parties that receive nonpublic personal information from a nonaffiliated financial institution can further use or disclose that information.[15] If a company receives information under certain GLBA exception—when the consumer does not have the right to opt-out—then reuse and redisclosure is generally limited to activities falling under the relevant exception.[16] In other cases, recipients can generally redisclose information only to the extent the originating financial institution could lawfully have done so.[17]

GLBA also requires financial institutions to send privacy notices to consumers, disclosing the financial institution's policies and practices for collecting nonpublic personal information and disclosing it to third parties.[18] The notices must be clear and conspicuous, and include the categories of personal information collected by the institution, the categories of persons with whom the information may be shared, and certain other disclosures. The notices also must be made in accordance with federal regulations. GLBA also required federal agencies to develop a voluntary model privacy form to provide financial institutions with a safe harbor under GLBA and to enable consumers to easily identify and

[13]15 U.S.C. § 6802(b)(2); 12 C.F.R. § 1016.13. *See also* 15 U.S.C. § 6802 (e)(1) and 12 C.F.R. § 1016.14

[14]15 U.S.C. § 6802(e)(6)(A), (e)(8); 12 C.F.R. § 1016.15.

[15]15 U.S.C. § 6802(c).

[16]Disclosures to certain affiliates are also permitted. 12 C.F.R. § 1016.11(a), (c).

[17]Disclosures to certain affiliates are also permitted. 12 C.F.R. § 1016.11(b), (d).

[18]15 U.S.C. § 6803. In general, financial institutions must provide an initial privacy notice when a consumer becomes a customer (for example, opens a new account), and annual notices thereafter for the duration of the customer relationship. Initial or annual notices may not be required in some cases, such as when disclosures are made only to process or service a transaction requested by the consumer or under other exceptions to GLBA's opt-out requirement. 12 C.F.R. §§ 1016.4-1016.6, 1016.8.

compare practices among financial institutions.[19] The model form was released in December 2009 and is discussed in more detail later in this report.

In addition to these provisions, which help to protect consumers' privacy, GLBA requires certain specified federal agencies to establish standards for financial institutions related to administrative, technical, and physical safeguards to ensure the security and confidentiality of customer records and information, protect against anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.[20]

GLBA's privacy and safeguards provisions—as they apply to banks and credit unions—are implemented by CFPB and the four prudential regulators. Specifically, GLBA's privacy provisions are implemented under CFPB's Regulation P, while the standards for protecting the security, confidentiality, and integrity of customer information are established by the four prudential regulators.[21]

Fair Credit Reporting Act Requirements

Enacted in 1970, FCRA governs the collection, use, and disclosure of personal information used to evaluate a consumer's eligibility for credit, insurance, and other purposes.[22] For example, this can include information regarding a consumer's creditworthiness, general reputation, and personal characteristics. Banks and credit unions may be subject to FCRA for a number of reasons, such as if they meet the definition of a consumer reporting agency, furnish information to consumer reporting

[19]Institutions that choose to use the model privacy form in accordance with its instructions will satisfy the disclosure requirements for privacy notices under GLBA and related content requirements under Regulation P (that is, they will obtain a "safe harbor" from a determination of noncompliance). 15 U.S.C. § 6803(e)(4); 12 C.F.R. § 1016.2(a).

[20]15 U.S.C. § 6801(b).

[21]Regulation P, 12 C.F.R. pt. 1016; Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 30, app. B, pt. 208, app. D-2, pt. 225, app. F, pt. 364, app. B; and Guidelines for Safeguarding Member Information, 12 C.F.R. pt. 748 app. A.

[22]Under FCRA, a consumer is any individual. 15 U.S.C. § 1681a(c).

agencies, or use information in consumer reports that consumer reporting agencies issue.[23]

FCRA helps to protect a consumer's privacy by limiting the disclosure and use of consumer reports to certain permissible purposes.[24] In addition, FCRA gives consumers the right to opt out of the sharing or use of their information among affiliated entities. For example, FCRA's affiliate marketing provision applies to institutions that use information from their affiliates for marketing solicitations or provide information to their affiliates for that purpose. In general, institutions may not use consumer information received from an affiliate to make a solicitation for marketing purposes, unless the consumer is notified and given an opportunity to opt out of receiving solicitations.[25] In addition, FCRA provides for notice and opt-out when affiliates share certain types of information regarding the consumer, regardless of the purpose for which it is shared.[26] GLBA's model privacy form is designed to incorporate FCRA's notice and opt-out requirements, where applicable. FCRA's privacy provisions are generally implemented under CFPB's Regulation V.[27]

[23]A consumer report is any communication of any information by a consumer reporting agency bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living that is used or expected to be used or collected as a factor in establishing the consumer's eligibility for credit or insurance primarily for personal, family, or household purposes, employment, or certain other authorized purposes. 15 U.S.C. § 1681a(d)(1). Certain communications among affiliates are excluded from the definition of a consumer report. *See*, e.g., 15 U.S.C. § 1681a(d)(2)(A)(ii)-(iii).

[24]15 U.S.C. § 1681b.

[25]If the consumer opts out, then the information may not be used for marketing solicitations. 15 U.S.C. § 1681s-3(a); 12 C.F.R. § 1022.21(a). There are certain exceptions to the notice and opt-out requirement, such as solicitations made to a consumer with whom the institution has a pre-existing business relationship. *See* 15 U.S.C. § 1681s-3(a)(4) and 12 C.F.R. § 1022.21(c).

[26]15 U.S.C. § 1681a(d)(2)(A)(iii). Sharing pursuant to this provision is reflected on GLBA's model privacy form as "For our affiliates everyday purposes—information about creditworthiness." According to Regulation P, an institution that shares for this reason must provide an opt-out. 12 C.F.R. pt. 1022, app., instruction C.2(d)(5). Additional privacy protections under FCRA includes restrictions on obtaining or using medical information to determine eligibility for credit, and sharing and redisclosure of medical information. 15 U.S.C. §§ 1681a(d)(3), 1681b(g) and 12 C.F.R. pt. 1022, subpt. D.

[27]12 C.F.R. pt. 1022.

CFPB and Prudential Regulators Implement and Enforce Federal Consumer Privacy Laws

CFPB has rulemaking authority to implement the federal consumer financial laws, including privacy requirements under GLBA and FCRA.[28] In addition, CFPB has supervisory and enforcement authority for federal consumer financial laws for insured depository institutions and insured credit unions with more than $10 billion in total assets, as well as their affiliates and certain nonbank financial institutions.[29] CFPB does not have rulemaking, supervisory, or enforcement authority in regard to GLBA's safeguards requirement.

The federal prudential regulators (FDIC, Federal Reserve, OCC, and NCUA) oversee their respective financial institutions for safety and soundness. As shown in table 1, the jurisdiction of each regulator depends on the type of charter an institution chooses (commercial bank, thrift, or credit union) and the origin of the charter (federal or state).

[28]Federal consumer financial laws also include Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act, the Equal Credit Opportunity Act, the Truth in Lending Act, the Fair Debt Collection Practices Act, certain other enumerated laws, and implementing regulations. 12 U.S.C. § 5481(14). CFPB's rulemaking authority is subject to certain exceptions. *See* 12 U.S.C. § 5517. With respect to GLBA's privacy requirements, CFPB's rulemaking authority does not extend to entities regulated by the Securities and Exchange Commission or Commodity Futures Trading Commission, certain motor vehicle dealers regulated by the Federal Trade Commission, and state-regulated insurance companies. 15 U.S.C. § 6804(a)(1); 12 C.F.R. § 1016.1(b)(1).

[29]12 U.S.C. §§ 5514-5516.

Table 1: Federal Prudential Regulators and Their Basic Functions

Agency	Basic function
Office of the Comptroller of the Currency	Charters and supervises national banks, federal thrifts, and federally chartered branches and agencies of foreign banks.
Board of Governors of the Federal Reserve System	Supervises state-chartered banks that opt to be members of the Federal Reserve System; bank and thrift holding companies, and the nondepository institution subsidiaries of those institutions; and nonbank financial companies designated by the Financial Stability Oversight Council for consolidated supervision and enhanced prudential standards. Supervises state-licensed branches and agencies of foreign banks and regulates the U.S. nonbanking activities of foreign banking organizations.
Federal Deposit Insurance Corporation	Supervises state-chartered banks that are not members of the Federal Reserve System, as well as state savings banks and thrifts; insures the deposits of all banks and thrifts that are approved for federal deposit insurance; has the authority to conduct backup examinations for any insured institution; resolves all failed insured banks and thrifts and, if appointed receiver by the Secretary of the Treasury, has authority to resolve certain large bank holding companies and nonbank financial companies.
National Credit Union Administration	Charters and supervises federally chartered credit unions and insures savings in federal and most state-chartered credit unions.

Source: GAO. | GAO- 21-36

The four prudential regulators also have supervisory and enforcement authority for the federal consumer financial laws with respect to insured depository institutions and insured credit unions with $10 billion or less in total assets, subject to their respective jurisdictions. In addition, the four prudential regulators have authority to establish, implement, and enforce GLBA's standards for safeguarding customer information for all institutions subject to their jurisdiction, regardless of size.

Banks and Credit Unions Collect, Use, and Share Personal Information, and Some Consumers May Be Unaware How Financial Technology Firms Use Their Information

Banks and credit unions collect extensive amounts of personal information and primarily use it to provide products and services, conduct everyday business activities, and market products and services to consumers. They also share personal information with third parties that help them conduct their business activities and marketing. Banks and credit unions are also required to have processes in place to protect the personal information they collect, use, and share with third parties. Financial technology services that help consumers access and manage all their financial information in one place present additional privacy risks to consumers, and banks and credit unions generally do not control how those companies use personal information.

Banks and Credit Unions Collect and Use Personal Information Primarily for Business Functions and for Marketing

Banks and credit unions collect and use many types of personal information to (1) conduct everyday business activities (see table 2) and (2) market products and services. Banks and credit unions collect personal information directly from consumers when they submit applications to open an account, apply for a loan or credit card, or seek advice about their investments. For example, banks and credit unions obtain a consumer's name and date of birth to verify the consumer's identity. Banks and credit unions also obtain personal information from consumer reporting agencies, affiliates, data brokers, and other companies. For example, they collect credit history information from consumer reporting agencies to determine eligibility for loans. The information may be used to create bank statements, monitor for fraud, determine credit eligibility, or determine whether to offer other products and services. Banks and credit unions also collect and use personal information to compile a customer profile that later can be used for marketing purposes.

Table 2: Consumer Personal Information That Banks Collect for Everyday Business Activities

Category	Data types
Identifying information	Name
	Social Security number
	Date of birth
	Physical address
	Phone number
	Email address
	Driver's license number
	Driver's license (scan)
Financial information	Credit/debit transactions and history
	Credit accounts/balances
	Consumer reporting agency information, including credit score
	Payment/bill history
	Financial assets
	Bank account statements
	Bank/financial accounts
	Information about investment account transactions
	Retirement portfolio information
	Mortgage information
	Pay stubs
	Tax forms, such as W-2 forms
	Insurance applications, payments, and claims
Employment information	Occupation
	Employment history
	Source of income
Other	Mother's maiden name/father's name
	Citizenship
	Marital status
	Tax advice/preparation
	Residence history
	Military service status

Source: GAO analysis of selected online applications of banks and credit unions for checking accounts and mortgages. | GAO- 21-36

Banks and credit unions also collect personal information that is gathered from consumers' online activity (see table 3). For example, the personal information that consumers provide in online forms and surveys may

include name, date of birth, and demographic information, such as age and gender.[30] Banks and credit unions also collect other information that may not identify an individual—such as social media activity, browsing activity and behavior, type of computer or mobile device, and network address—when consumers access the financial institution's website and use mobile or online services. For example, officials from one bank stated that they may use information about social media activity to deliver targeted advertisements to their customers. According to the online privacy policies of the largest banks and credit unions we reviewed, the primary purposes for collecting information online include ensuring that their websites function properly, detecting and preventing fraud, maintaining website security, and tailoring advertisements based on the individual's browsing behavior.[31]

Table 3: Consumers' Online Information That Banks and Credit Unions Collect from Their Websites

Category	Data types
Online behavior	Social media activity/behavior
	Browsing activity/behavior
Information gathered from online session during account log-on	Cookies
	Location (ZIP code)
Information associated with individual's device	Computer identifying information
	Internet protocol address
	Browser information
	Mobile device model
Information obtained from online forms, applications, and surveys	Name
	Postal or email address
	Phone number
	Account numbers
	Date of birth
	Demographic information, such as age and gender
	Household income

Source: GAO analysis of bank and credit union online privacy notices. | GAO- 21-36

[30]The collection of information about a borrower's personal characteristics is subject to the Equal Credit Opportunity Act. *See* 15 U.S.C. §§ 1691-1691f and 12 C.F.R § 1002.5.

[31]These online privacy policies are separate from the privacy notices required under GLBA. In some cases, these additional disclosures may be required by state law. *See*, e.g., California Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-579.

Banks and Credit Unions Share Personal Information with Service Providers and Others for Several Purposes

Banks and credit unions share personal information with various types of third parties (see table 4). These include service providers, which banks and credit unions rely on to help them fulfill everyday business functions and to market products and services. For example, for everyday business purposes, bank officials we interviewed said they share information with service providers to process customer transactions, maintain accounts, respond to court and legal investigations, and report to consumer reporting agencies. In addition, banks and credit unions may contract with service providers to deliver products and services. For example, bank officials we interviewed said they contract with a check printing service to print and deliver checks to the bank's customers.

Table 4: Types of Third Parties with Which Banks and Credit Unions May Share Consumer Information

Affiliate	Companies related by common ownership or control.
Nonaffiliate	Companies not related by common ownership or control.
Financial companies	Mortgage bankers, securities brokers-dealers, and insurance agents, among others.
Nonfinancial companies	Retailers, magazine publishers, airlines, and direct marketers, among others.
Service providers	Companies that deliver services to or perform functions on behalf of the institution.
Other organizations	Government agencies and nonprofit organizations, among others.

Source: GAO analysis of Regulation P (12 C.F.R. pt. 1016). | GAO- 21-36

Banks and credit unions also have legal obligations to maintain and report certain personal information that they collect to prevent fraud and other misconduct.[32] For example, credit unions must collect information to verify qualification for membership in a particular credit union's field of membership (that is, its basis for eligibility). According to a credit union industry group we interviewed, for a credit union with a field of membership based on a community bond, credit unions must collect residential or professional addresses to establish that consumers live or work in that designated community.

[32]Banks and credit unions may continue to retain their information to meet legal requirements, even after an individual is no longer a customer.

Other examples of legal obligations that banks and credit unions must meet include the following:

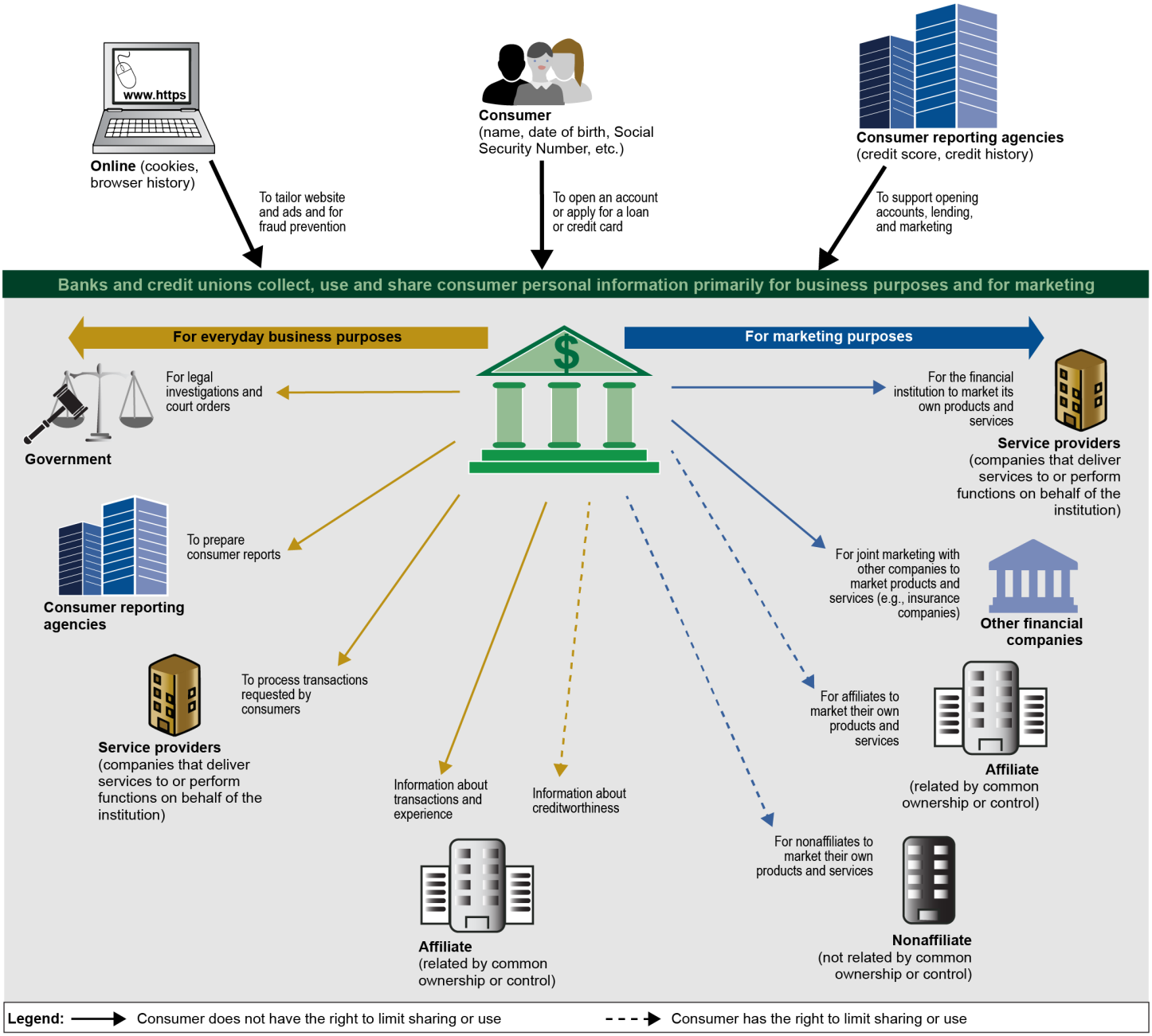
- Reporting certain payments made by customers to foreign entities and related tax withholdings, pursuant to the Foreign Account Tax Compliance Act.
- Collecting and maintaining a customer's name, date of birth, address, Social Security number, and details of large financial transactions under Bank Secrecy Act regulations.
- Submitting suspicious activity reports to the Financial Crimes Enforcement Network to help combat money laundering and other illicit activities under the Annunzio-Wylie Anti-Money Laundering Act.

Furthermore, most banks and credit unions share customer information with consumer reporting agencies, including transaction history, payment history, and information about whether the consumer paid on time, and if late, any collection activity, or if the consumer closed an account. They share this information so that consumer reporting agencies can assemble or evaluate it and compile consumer reports. Banks and credit unions may use consumer reports to determine consumer eligibility for products and services such as credit and insurance.

Banks and credit unions also may share customers' personal information (including information related to their purchases) with affiliates to market products and services to their customers (see fig. 1). For example, a credit union might share a list of its customers and their credit scores with an affiliate, such as a credit union service organization.[33] Banks and credit unions also may share information with nonaffiliated companies that market their own products and services to those customers. For example, officials from a large bank said it partners with another company to offer an affinity rewards program in which customers can earn travel rewards. The bank shares information about account holders' transactions with its partner company so that rewards can be credited to individuals, but this company also may market its products and services to the bank's customers.

[33]In general, a credit union service organization is an entity that is wholly or partially owned by a federally insured credit union (or that has received a loan from a federally insured credit union) and that is engaged primarily in providing products and services to credit unions or credit union members.

Figure 1: Summary of Bank and Credit Union Data Sharing



Source: GAO analysis of banks' and credit unions' privacy notices and related regulations. | GAO-21-36

Officials from banks we interviewed stated that they share certain consumer transaction information with third-party vendors that manage and email the banks' marketing material to customers. For example, when individuals buy a house or car, they may receive mail offers to refinance their loan or purchase a vehicle warranty. In such cases, the bank or credit union sends a list of purchasers to the marketing vendor. The vendor then makes a selection and sends back a list to the bank or credit union, which in turn provides the vendors with email addresses and names so they can market directly to those individuals.

Nonaffiliated companies with which banks and credit unions may share consumer data, such as credit card lenders and some mortgage brokers, use information about a consumer's transaction and payment history for prescreening, a method of selecting consumers who meet certain criteria (such as individuals with a specific credit score range and mortgage balance living in a specified ZIP code) for the purpose of making credit offers. In another example, a consumer advocacy group we interviewed stated that when a consumer applies for a mortgage, an alert will go out to other mortgage brokers so they can offer other products or services, such as a credit card. According to a bank official, in such cases, both the bank and the nonaffiliated company may benefit from marketing a particular product. For example, an automobile dealer may make an offer to a bank customer based on information the bank shared about the customer's financial activity.

Banks and Credit Unions Are Required to Safeguard Nonpublic Personal Information

As discussed earlier, banks and credit unions are required to safeguard nonpublic personal information. Regulatory guidelines require banks to design an information security program for protecting customer information to control the risks that they have identified through a risk assessment.[34] According to bank officials we interviewed, processes they use to protect customer information include conducting physical security checks, performing vulnerability testing, and having other internal control processes for reporting security breaches, managing records, and documenting the control environment. They also conduct data security risk assessments with all third parties under contract with the bank or credit union to ensure that nonpublic personal information is protected and is not being used outside of the contracted terms and intended purposes.

[34] *See*, e.g., 12 C.F.R. pt. 30, app. B.

Bank officials we interviewed stated that their standard risk-management framework serves as a control for managing their financial privacy risks. According to annual reports of some of the banks that we reviewed, the risk-management frameworks offer “three lines of defense”: front-line units, independent risk management, and an internal audit function.

- Front-line units constitute the first line of defense, in which executive-level management is responsible for managing risks across business lines and for implementing a risk-management structure. These units also help ensure that banks and credit unions adhere to applicable laws, rules, and regulations.
- Independent risk management constitutes the second line of defense. It is independent of bank and credit union business lines, and assesses risks across business activities and challenges the risk-management practices of the front-line units. The risk-management group also is responsible for the development of policies and procedures that outline how risks are identified, measured, monitored, and controlled.
- The internal audit function of a bank is the third line of defense. It operates independently from the other two lines of defense and from other parts of the banks and credit unions. The corporate general auditor performs independent testing and evaluation of key processes and controls across business lines.

Officials from the banks we interviewed also stated that they have processes in place to continually monitor and oversee third parties to ensure that they honor customers’ requests to opt out of having their information shared for marketing purposes. The officials stated they have staff who verify that third parties have honored opt-out requests from customers.

Consumers May Be Unaware of How Financial Technology Applications Use Personal Information and the Associated Privacy Risks

While banks and credit unions are required to protect the personal information they collect, some of the banks and industry and consumer groups told us the increased use of financial technology applications (fintech apps) may put this personal information at risk. Consumers may be largely unaware of how fintech apps use their personal information and the privacy risks that such usage poses. During a panel discussion at a 2020 CFPB symposium, a fintech company stated that more than 100 million U.S. consumers use fintech apps to facilitate activities such as

payroll direct deposit, bill payment, investing, and saving.[35] In particular, fintech companies that rely on companies known as data aggregators offer products that allow individuals to consolidate all their accounts from multiple financial institutions so they can view all their account information in a centralized location. To use such services, a consumer typically downloads an app to a computer or mobile device and provides login credentials to the app so it can access and aggregate financial information from the consumer's bank or credit union accounts.

Stakeholders who represent large banks, fintech companies, and consumer advocacy groups have expressed several concerns regarding the use of data aggregators. A representative from a large bank stated that data aggregators enable fintech apps to link customer bank accounts to their platform so these apps can offer customers various financial services and tools to manage their personal finances, such as making person-to-person payments and budgeting. Three large banks identified multiple risks with this type of consumer-authorized data access. Specifically, banking representatives stated that consumers are not fully aware that data aggregators store their banking credentials indefinitely and obtain a consumer's financial data by acting as the consumer and entering their credentials to access their financial account information online. This access could give the data aggregator the ability to take any action as the consumer, such as initiating electronic funds transfers and account changes. Industry and consumer privacy groups we interviewed also stated concerns that consumers using data aggregators may be unaware of who collects their sensitive financial information, how it is collected, how long it is stored, and with whom it is shared. According to a 2019 consumer survey, 80 percent of about 4,000 users of a banking app were not fully aware that apps or third parties may store their banking credentials.[36]

To address these concerns, officials from four banks we interviewed stated that they have been developing application programming

[35]The symposium, "Consumer Access to Financial Records," was held in Washington, D.C., on February 26, 2020.

[36]The Clearing House, *Consumer Survey: Financial Apps and Data Privacy* (November 2019).The criteria for selecting survey participants included use of mobile or online banking. Any respondents who did not use credit or debit cards, mobile wallets, or person-to-person payment providers were removed from the survey population. The second half of the survey included only respondents who used fintech apps in the past year. Survey results may not be generalizable to the U.S. population that uses online or mobile banking and fintech apps.

interfaces intended to provide a more secure way for fintech apps to connect and access consumers' bank accounts. The interfaces need to be developed in collaboration with fintech companies to ensure they function properly and securely. The interfaces will redirect customers to the banks' secure websites, where customers are prompted to enter their login credentials (rather than providing the credentials directly to the apps). Representatives from a credit union industry group we interviewed stated that, while interfaces are useful tools, they are best used in combination with a bilateral agreement between the financial institution and fintech company that clearly delineates which entity is liable for misuse of transferred data.

Banks and credit unions generally do not control information that is shared under separate arrangements that consumers may make with fintech companies. While fintech services and applications can provide consumers with convenient means to manage their finances, they present risks to consumers because there often is no direct contractual relationship between the fintech companies and the banks or credit unions used by the consumer. The online privacy policies of the banks and credit unions that we reviewed state that they have no control over the privacy, security, or accuracy of information these fintech apps may maintain. Instead, the banks and credit unions stated that the fintech companies follow their own privacy and data security policies.

We previously found in a 2018 report that fintech firms not partnered with banks or credit unions typically would not be subject to routine examinations by a federal financial regulator; instead, they would be subject to state regulatory oversight and enforcement.[37] In 2017 CFPB released consumer protection principles for market participants to consider in relation to use of fintech apps that aggregate consumer data.[38] These principles are intended to safeguard consumer interests in this market, but as we reported in 2018, these principles are not set forth in regulation and therefore are not legally binding. We recommended that CFPB engage in collaborative discussions with other relevant financial regulators and other stakeholders to address issues related to consumers' use of account aggregation services. CFPB agreed with our

[37]GAO, *Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight*, GAO-18-254 (Washington, D.C.: Mar. 22, 2018).

[38]Consumer Financial Protection Bureau, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* (Washington, D.C.: Oct. 18, 2017).

recommendation. Since our report was issued, CFPB held a symposium on consumer access to financial records that included a panel representing large banks, fintech companies, and consumer advocacy groups and discussed the current landscape and benefits and risks of consumer-authorized data access by third parties. The symposium was intended to inform CFPB's policy development process, including possible future rulemakings. Following the symposium, on July 24, 2020, CFPB announced that it planned to issue an advance notice of proposed rulemaking later in 2020 on consumer-authorized access to financial records. We continue to monitor steps CFPB has taken to address our recommendation.

Privacy Notices Provide Limited Insight into How and with Whom Banks and Credit Unions Share Consumer Personal Information

In 2009, federal agencies issued a model privacy form as required under GLBA, which banks and credit unions widely adopted. The model form relies heavily on standardized language, and requires institutions to disclose only a small number of categories of personal information they collect and the ways they use it. As a result, the model form provides consumers with limited insight into the specific information that banks and credit unions collect and with whom they share it. While the model form represents an improvement over earlier privacy notices that were often too difficult for consumers to read and understand, it may now be out of date.

Federal Regulators Developed a Model Privacy Form That Banks and Credit Unions Widely Adopted

Development of Model Privacy Form

The Gramm-Leach-Bliley Act model privacy form was developed in three phases:

In phase 1, federal financial regulatory agencies contracted with a communication research company to develop a prototype privacy notice. The prototype was based on qualitative research, including interviews with consumers.

In phase 2, the agencies contracted with another company to assess the effectiveness of the prototype notice against three alternative notices by testing it with a larger group of consumers. The testing assessed and compared the notices' ability to help consumers compare information collection and sharing practices among banks, evaluate the opt-out choices described in the notices, and make informed choices among banks. The results of this study prompted changes to the prototype notice, which were later validated through additional testing.

In phase 3, the communication research company developed and validated designs for incorporating opt-out options at the bottom of the notice's first page. The testing validated that the table format was consumer friendly and that moving certain information to the first page was important.

Source: GAO analysis of the model privacy form development studies. | GAO- 21-36

In 2004, federal agencies, including FDIC, the Federal Reserve, OCC, and NCUA, began a multiphase project to develop a model privacy form.[39] GLBA specified that the model privacy form must be comprehensible to consumers, provide for clear and conspicuous disclosures, enable consumers to easily identify sharing practices and compare privacy practices among financial institutions, and be succinct.[40] Prior to this effort, the agencies found that some financial institutions' privacy notices incorporated lengthy statements of terms and conditions, making it harder for consumers to find information about privacy practices and raising questions about whether such notices complied with the requirement that they be clear and conspicuous.[41] The final model privacy form was issued in 2009, after a long development and testing process (see sidebar). The form, which consists of two pages, was initially paper-based, but was later converted to a web-based version.

The form's first page contains information about what type of personal information the financial institution collects, why that information is shared, the extent to which consumers can limit sharing (opt out), and the methods for doing so. The second page contains information about how the financial institution protects a consumer's personal information, how the information is collected, why consumers cannot limit all sharing, and information on limiting sharing for joint account holders. In addition, it includes definitions of affiliates, nonaffiliates, and joint marketing, as well as other information as permitted under Regulation P.

The form's standardized language allows users to easily compare privacy practices across financial institutions. Banks and credit unions can only customize the model privacy form in limited ways, such as choosing examples of third parties with whom they share information and adding disclosures required under state laws. If a bank or credit union modified the model privacy form other than as permitted under Regulation P, it would not qualify for the safe harbor under GLBA.[42] Although the use of

[39]Prior to the transfer of authority under the Dodd-Frank Wall Street Reform and Consumer Protection Act, rulemaking authority for GLBA's privacy provisions was shared among these and other regulators.

[40]15 U.S.C. § 6803(e)(2).

[41]The agencies also found that some institutions included vague assurances to consumers that implied their personal information was not shared broadly, while obscuring or directing attention from disclosures of actual information-sharing practices.

[42]12 C.F.R. pt. 1016 app., instruction B.1(b).

the model privacy form is voluntary, it has been widely adopted within the industry.

Model Privacy Form Limits the Extent to Which Banks and Credit Unions Disclose Their Collection and Sharing of Personal Information

As noted earlier, GLBA requires that banks and credit unions provide consumers with clear and conspicuous notice of the institution's policies and practices for collecting and sharing nonpublic personal information. Banks and credit unions generally use the GLBA model privacy form to comply with GLBA's notice and opt-out requirements because doing so enables them to obtain a safe harbor for compliance purposes. However, the continued proliferation of consumer data sharing suggests the form may be out of date and may not accurately represent the increased and varied ways financial institutions share information compared to when the form was implemented over 10 years ago.

Limited Disclosure of What Information Is Collected

While the current model form is more readable than privacy notices previously used by financial institutions, it discloses only a small number of the types of personal information they collect and share and the ways in which the information is collected. For example, Regulation P identifies 24 types of consumer personal information institutions may collect and share, but the form only includes six types: one that is mandatory (Social Security number) and five to be selected by the institution.[43] Furthermore, the regulation identifies 34 examples of how banks and credit unions may

[43]The 24 types of personal information identified in Regulation P are Social Security number; income; account balances; payment history; transaction history; transaction or loss history; credit history; credit scores; assets; investment experience; credit-based insurance scores; insurance claim history; medical information; overdraft history; purchase history; account transactions; risk tolerance; medical-related debts; credit card or other debt; mortgage rates and payments; retirement assets; checking account information; employment information; and wire transfer instructions. 12 C.F.R. pt. 1016 app., instruction C.2(b).

collect personal information from consumers, but the form only discloses five of those examples.[44]

Institutions may customize this part of the model form only where terms or spaces are shown in brackets (as illustrated in fig. 2) by selecting from the menu of terms provided in the regulation. Figure 2 shows the GLBA model privacy form template with five predefined types of personal information that institutions collect and share, and five predefined ways in which they collect the information from consumers.

Figure 2: Excerpts of the Gramm-Leach-Bliley Act Model Privacy Form Showing Predefined Examples

What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How does [name of financial institution] collect my personal information?	We collect your personal information, for example, when you ■ **[open an account]** or **[deposit money]** ■ **[pay your bills]** or **[apply for a loan]** ■ **[use your credit or debit card]** [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]

Source: Gramm-Leach-Bliley Act Model Privacy Form. | GAO-21-36

[44]The 34 examples of how (or when) financial institutions collect personal information are when consumers open an account; deposit money; pay their bills; apply for a loan; use their credit or debit card; seek financial or tax advice; apply for insurance; pay insurance premiums; file an insurance claim; seek advice about their investments; buy securities from the institution; sell securities to the institution; direct the institution to buy securities; direct the institution to sell their securities; make deposits or withdrawals from their account; enter into an investment advisory contract; give their income information; provide employment information; give their employment history; tell the institution about their investment or retirement portfolio; tell the institution about their investment or retirement earnings; apply for financing; apply for a lease; provide account information; give their contact information; pay the institution by check; give their wage statements; provide their mortgage information; make a wire transfer; tell the institution who receives the money; tell the institution where to send the money; show their government-issued ID; show their driver's license; or order a commodity futures or option trade. 12 C.F.R. pt. 1016, app., instruction C.3(a)(3).

In the privacy notices we reviewed, banks and credit unions generally included examples of ways in which they collect consumer data that were the same as the predefined examples in the model privacy form. A 2016 study that evaluated use of the GLBA model privacy form by more than 6,000 banks and credit unions found a similar pattern, with many predefined examples that were taken from the model form rather than customized.[45]

In our analysis of 60 bank and credit union GLBA model privacy notices, we found that 12 used only predefined examples of the types of personal information collected.[46] In other cases, institutions selected predefined examples (account balance and credit history) as well as other categories (such as employment information, transaction history, and investment experience) from the menu in the regulation.

Furthermore, 22 banks and credit unions used the predefined examples for how they collect information, and 37 used a combination of the predefined examples and additional terms from the menu in the regulation.[47] For example, some institutions selected predefined examples (such as "open account," "apply for a loan," and "use credit or debit card") and terms from the menu (such as "seek advice about your investments" and "make deposits and withdrawals from your account").

Limited Disclosure about with Whom Information Is Shared

The model privacy form describes the reasons why banks and credit unions share personal information and whether consumers can opt out of such disclosures. As discussed earlier, consumers have the right to limit some, but not all, sharing of personal information. According to consumer advocacy groups and an industry group we interviewed, the consumer opt-out rate is generally low. Some of the banks we interviewed

[45]Lorrie Faith Cranor, Pedro Giovanni Leon, and Blase Ur, *A Large-Scale Evaluation of U.S. Financial Institutions' Standardized Privacy Notices*.

[46]Of the 12 banks and credit unions that used the predefined examples of personal information on the model privacy form, three were institutions with total assets of over $10 billion and nine had total assets of $10 billion or less.

[47]Of the 22 banks and credit unions that used the predefined examples of methods, 10 were institutions with total assets of over $10 billion and 12 had total assets of $10 billion or less. Of the 37 banks and credit unions that customized their selection of methods, 19 were institutions with total assets of over $10 billion and 18 had total assets of $10 billion or less.

corroborated this observation, noting that opt-out rates were mostly low but varied.[48]

As seen in table 5, very few institutions offered consumers the right to opt out of sharing or use beyond what is required by law (that is, the purposes in the last three rows of the table). In addition, sharing practices varied among banks and credit unions. All 60 institutions (100 percent) share with third parties for everyday business purposes, 52 of 60 (87 percent) share with service providers for marketing purposes, and 43 of 60 (72 percent) share in other ways, such as for joint marketing purposes. Where consumers have a right to opt out by law, 32 of 60 institutions (53 percent) share with affiliates for marketing purposes; 28 of 60 (47 percent) share credit-related information with an affiliate for everyday business purposes; and eight of 60 (13 percent) share with nonaffiliates for marketing purposes.

Table 5: Disclosure of Information-Sharing and Opt-Out Provisions of 60 Selected Banks and Credit Unions That Use the Model Privacy Form

	Institutions with over $10 billion in assets		Institutions with $10 billion or less in assets	
Reason for sharing personal information	**Number of institutions that share**	**Number of institutions that offer opt-outs**	**Number of institutions that share**	**Number of institutions that offer opt-outs**
For everyday business purposes—such as to process transactions, maintain accounts, respond to court orders and legal investigations, or report to consumer reporting agencies	29	0	31	0
For marketing purposes—with service providers to offer products and services	28	3	24	2
For joint marketing with other financial companies	22	1	21	1
For affiliates' everyday business purposes—information about transactions and experiences	27	1	16	1
For affiliates' everyday business purposes—information about creditworthiness	19	19	9	9

[48]Three banks we interviewed said their opt-out rates were less than 5 percent, and three other banks said their opt-out rates ranged from 7 to 32 percent.

Reason for sharing personal information	Institutions with over $10 billion in assets		Institutions with $10 billion or less in assets	
	Number of institutions that share	Number of institutions that offer opt-outs	Number of institutions that share	Number of institutions that offer opt-outs
For affiliates to market to customers	21	21	11	11
For nonaffiliates to market to customers	7	7	1	1

Source: GAO analysis of bank and credit union privacy notices. | GAO- 21-36

Note: We selected 29 institutions with total assets of more than $10 billion and 31 institutions with total assets of $10 billion or less. These institutions adopted the model privacy form to comply with notice and opt-out requirements under the Gramm-Leach-Bliley Act.

Neither GLBA nor Regulation P expressly requires banks and credit unions to disclose in their privacy notices or elsewhere a full list of all the specific parties with which they share personal information. Instead, banks and credit unions are only required to disclose the categories of affiliates and nonaffiliates with whom they share information (such as financial companies or nonfinancial companies), together with a few illustrative examples (such as mortgage bankers and retailers) as applicable.[49]

In our review of the 60 privacy notices, we found that banks varied in how much information they disclosed about their affiliates and nonaffiliates. A majority of the notices we reviewed disclosed examples of the affiliated companies with which they shared personal information. Some banks' notices stated that their affiliates include companies whose names incorporated the name of the bank, and one bank stated that its affiliates can be financial and nonfinancial companies but did not provide any examples. One large bank that we reviewed provided on its website a link to a list of its affiliate companies. Another large bank provided a link to a list of its affiliate companies only in its international privacy policy.[50] The bank said other countries where it conducts business require the bank to identify all affiliates. Other large banks provided a list of their affiliate

[49]15 U.S.C. § 6803(c)(1)(A); 12 C.F.R. § 1016.6(a)(3) and (c)(3). *See also* 12 C.F.R. pt. 1016, app. instruction C.3(b).

[50]As noted earlier, banks and credit unions may be subject to international laws, such as the General Data Protection Regulation, which imposes general data privacy protections outside of the United States. As we previously reported, European Union officials said that the General Data Protection Regulation's jurisdiction is expansive and can cover all entities—including those based in the United States—that process data in the European Union or engage in business that affects people within the European Union. GAO, *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses,* GAO-20-522 (Washington, D.C.: July 13, 2020).

companies in their 10-K filings to the Securities and Exchange Commission, which are comprehensive annual reports for investors about financial performance that publicly traded companies must file and may include affiliates that have no relationships with retail customers. In contrast, most or almost all of the smaller banks and credit unions (those with assets of $10 billion or less) generally do not share information with affiliates in contexts requiring consumer notice and the right to opt out.

Eight institutions reported sharing information with nonaffiliates for marketing purposes and disclosed categories of entities such as retailers, insurance companies, and direct marketing companies. For example, one bank that we interviewed said that it has about a dozen nonaffiliates, and its privacy notice discloses categories of companies such as retailers, auto dealers, and membership clubs. In another example, a credit union notice stated that its nonaffiliates can be financial and nonfinancial companies, but did not provide any examples. Thirty of the 31 smaller banks and credit unions we reviewed did not share personal information with nonaffiliates. Regulatory officials told us that these institutions, unlike larger ones, generally do not share information with nonaffiliates, apart from the contexts (described earlier) not subject to GLBA's opt-out requirement.

One reason the model privacy form provides limited information is that GLBA required it to be succinct and to enable a consumer to easily identify and compare practices across financial institutions. Prior to the development of the model form, privacy notices disseminated by financial institutions were considered to be difficult for consumers to read and understand. In addition, banks and credit unions may hesitate to provide more information on the form because doing so could disqualify them from receiving the "safe harbor" under GLBA. Officials from one bank told us they are limited in customizing their privacy notice because they do not want to lose the safe harbor it offers.

While the model form represents an improvement over earlier privacy notices, it may now be out of date. Guidance from NIST aimed at assisting federal agencies in protecting personal information in their custody states that notices of new information collections and details regarding how personal information will be used and protected are central

to providing individuals with privacy protections and transparency.[51] In addition to our analysis that found the form provides limited information, experts from consumer privacy groups and one industry group we interviewed said the GLBA model privacy form does not give the consumer a full explanation of what information banks and credit unions collect and how they share that information. Similarly, officials from three banks we interviewed said that the model form could be improved and be more transparent about how consumers' personal information is used and shared. Without a more complete disclosure of the ways in which banks and credit unions collect and share personal information, consumers may be unable to make informed decisions about protecting their information. Developed more than 10 years ago, the form was designed as a paper notice that financial institutions would mail to consumers. Although the form is now offered online, the design of the form has not been adapted to fully utilize online capabilities and features. For example, web-based notices would not have the same physical constraints as paper notices and could be designed to highlight key disclosures concisely but offer more detailed disclosures for those interested, using links or other features.

The limited information provided in the GLBA model privacy form, and the continued proliferation of consumer data shared since the form's implementation in 2009, suggests that a reassessment of the form is warranted. The prudential regulators last evaluated the model form over 10 years ago when it was finalized. Since that time, Congress transferred rulemaking authority for GLBA's privacy requirements to CFPB, which has not reassessed whether the form continues to meet consumer expectations for a clear and comprehensible disclosure of what information is shared and with whom. The agency has not determined whether the general increase in awareness and concern among consumers about their privacy merits different or more complete disclosures about the collection and sharing of their personal information. CFPB officials stated that they had not considered a reevaluation of the model form because they had not heard concerns regarding the privacy notice from industry or consumer groups, which are sources of information CFPB uses to prioritize regulatory and supervisory actions.

[51]National Institute of Standards and Technology, *Guide to Protecting the Confidentiality of PII,* NIST Special Publication 800-122 (Gaithersburg, Md.: April 2010). While the guide was prepared for use by federal agencies, nongovernmental organizations may also use it. Tasked with promoting U.S. innovation and competitiveness, NIST is responsible for the development of technical, physical, administrative, and management standards, including guidelines for the security and privacy of sensitive information.

However, our discussions with consumer and privacy groups showed that such concerns exist. Furthermore, technological advances in how information is organized and made available in a web-based model form could allow for a more detailed and comprehensive disclosure without sacrificing readability. An update to the model privacy form could result in banks and credit unions providing consumers with a more comprehensive understanding of the ways that these institutions collect, use, and share their personal information.

Regulators Generally Assessed Risk of Noncompliance Related to Financial Privacy as Low and Found Few or Minor Violations

CFPB and the prudential regulators have the authority to examine banks and credit unions for compliance with privacy requirements under GLBA, FCRA, and related regulations. However, from the 5 most recent years of completed examinations, the majority of the examinations did not include modules focusing on financial privacy requirements because the regulators did not identify an elevated compliance risk in these areas for the banks and credit unions examined during that time frame.[52] Regulators mostly found only minor privacy violations and consumer complaints related to these requirements. The prudential regulators also examine how banks and credit unions manage risks from third-party relationships as part of their examinations for safety and soundness but similarly have not focused on financial privacy.

Regulators Have Not Routinely Conducted Compliance Examinations on Financial Privacy

In conducting examinations, the prudential regulators and CFPB have processes to assess an institution's risk areas. Based on those assessments, the regulators generally have not conducted additional examination activity in the area of financial privacy because they have found it to be an area of low compliance risk. As a result, compliance in this area has usually been assessed at a more general level as part of the overall examination of compliance with federal consumer financial laws and regulations.

Prudential Regulators' Pre-Examination Risk Assessment and Planning

Examiners for the prudential regulators—FDIC, Federal Reserve, OCC, and NCUA—said that they routinely consider institutions' compliance with financial privacy laws and regulations as part of their risk-assessment and examination-prioritization process. Consumer compliance examiners conduct risk assessments and review planning as part of their compliance management review of banks and credit unions. They use the risk assessments and other planning activities to determine the scope of additional examination activities and whether to include modules related

[52]These modules consist of the Privacy of Consumer Financial Information Examination Procedures and the FCRA Regulation V Examination Module 2—Obtaining Information and Sharing among Affiliates. See appendix I for more details.

to financial privacy. They said that the approach includes consideration of factors such as an institution's asset size, relationships with affiliates and nonaffiliates, sharing practices, record of compliance, changes to its information collection and use practices since the previous examination, and trends in consumer complaints.

According to agency officials and documents, during the review planning phase, examiners create an institutional risk profile based on preliminary analysis of information and documents they receive from banks and credit unions and on discussions with management officials. For example, examiners submit a preexamination questionnaire or information request to banks and credit unions. Typically, examiners ask for bank and credit union internal policies and procedures (for delivering notice to customers, managing consumer opt-out directions, and preventing unlawful disclosure and use of account numbers and information from nonaffiliated financial institutions); information-sharing agreements with affiliates and service agreements or contracts with nonaffiliated third parties; categories of nonpublic personal information collected, used, and shared; and complaint logs.

Examiners also obtain internal audit reports and board meeting notes. For example, agency staff told us that if an examiner reviews an institution's general compliance management system and identifies compliance, procedural, or other weaknesses related to financial privacy provisions, then the examiner would look at those issues more closely. Examiners also incorporate any concerns raised during their ongoing supervision of banks and credit unions to determine if they apply to any aspects of the examination modules related to financial privacy. (We discuss examination modules later in this section.)

Finally, agency officials stated that examiners review their complaint database to identify any potential concerns for a bank or credit union that may warrant additional examination work. More specifically, they use data on consumer complaint activity when scoping and conducting examinations. They also use these data during their supervisory processes (for example, when monitoring financial institutions).

CFPB's Risk-Prioritization Process

According to CFPB information, to determine which product lines, institutions, and consumer compliance issues to examine for the larger institutions, CFPB determines the institutions and consumer product lines that pose the greatest risk to consumers, and prioritizes these for examinations annually. CFPB segments (tiers) the consumer product market into institution product lines, or specific institutions' offerings of

consumer product lines. CFPB then assesses the risk to consumers of each institution's product line at the market and institutional levels. CFPB uses the risk-tier assessments and other information—including from subject matter experts, recent legal and policy decisions that could affect examinations, and consultations with internal stakeholders—to develop its supervision strategy.

CFPB then uses the risk tiers and information from its supervision strategy to identify potential institutions for examination. After identifying institutions and product lines to examine, CFPB determines specific areas of compliance to assess by considering sources such as consumer complaints, public filings and reports, and past examination findings related to the same or similar products or institutions.

Financial Privacy Examinations Are Not Routine

Officials at FDIC, Federal Reserve, OCC, and NCUA told us that between 2014 and 2018, they did not routinely conduct transaction testing in the area of financial privacy. The reason for this, according to regulators, was that for most institutions they found no elevated compliance risks in the areas covered by these laws and regulations. An example of an elevated compliance risk, according to FDIC officials, would be if a bank had materially changed in its financial privacy practices since its last examination. In such a case, officials said the examiners would gather information on how the bank was mitigating any increased risk associated with those changes, such as through its oversight practices, policies, procedures, training, monitoring, and auditing. Examiners would use this information to assess whether transaction testing should be included as part of the examination. Additional information on these examination procedures is presented in appendix I.

Examiners at the prudential regulators also noted that mid-size and small community banks and credit unions present low risks to financial privacy because they generally do not share information in contexts requiring consumer notice and the right to opt out. However, the regulators told us they do routinely examine for compliance with GLBA's standards for safeguarding customer records and information.

CFPB examiners also told us that they have not routinely conducted specific examinations or transaction-level testing of compliance with financial privacy regulations for the banks and credit unions under CFPB jurisdiction. As with the prudential regulators, CFPB said the reason for

this was that its risk-prioritization assessments usually determined that the bank's risk in this area was low.[53]

Privacy Violations Identified Were Mostly Minor and There Were Few Consumer Complaints

The prudential regulators collectively oversee and examine over 10,000 banks and credit unions, and CFPB oversees and examines 150 of the largest institutions for compliance with federal consumer financial laws. While few examinations we reviewed from the 5 most recent years available (2014–2018) included transaction testing in the area of financial privacy, those that did mostly found violations that were relatively minor.[54] During this period, FDIC, NCUA, the Federal Reserve, and OCC found 141, 70, 19, and 17 banks, respectively, to be in violation of Regulation P; CFPB found one bank to be in violation of Regulation P. In some cases, these violations resulted in informal enforcement actions.[55] From 2014 through 2018, OCC found one bank with a violation related to Regulation V (covering affiliate disclosures), and the other regulators found none.

Table 6 lists examples of the violations among the 23 examinations we reviewed. The Regulation P violations varied but mostly consisted of technical mistakes and insufficient procedures and deficiencies related to oversight management and training.

[53]The CFPB does routinely examine for compliance with provisions in FCRA and Regulation V relating to accuracy, dispute handling and resolution, permissible purpose, and furnishing.

[54]The Federal Reserve, OCC, NCUA, and CFPB were unable to search specifically for Regulation P and Regulation V examinations in their databases and queried their databases for related violations. We therefore do not have the number of Regulation P and Regulation V examinations conducted.

[55]Regulators may use an informal enforcement action when a financial institution's overall condition is sound, but it is necessary to obtain written commitments to ensure that identified problems and weaknesses are corrected. Agreement to an informal action can be evidence of a commitment to correct identified problems before they adversely affect an institution's performance or cause further decline in its condition. Informal enforcement actions include commitment letters, deficiency letters, and memorandums of understanding.

Table 6: Examples of Violations of Regulation P from Examinations GAO Reviewed

➢ Bank had a broken hyperlink for a privacy notice, which resulted in failure of bank to provide notices to consumers.
➢ Bank's initial privacy disclosure did not contain the language required by the regulation, and in some instances, contained incorrect language.
➢ Bank incorrectly stated in privacy notices that the bank can collect and share checking account information with nonaffiliated third parties, but this is prohibited by regulation.
➢ Some bank customers who opted out of personal information sharing with a nonaffiliated third party were still included in the third party's marketing programs.
➢ Bank failed to provide an accurate initial privacy notice before disclosing nonpublic personal information to a nonaffiliated third party. Bank had a lapse in oversight of the joint marketing agreement with the third party, contributing to a release of customer account numbers to the third party.
➢ Credit union sold nonpublic information for joint marketing purposes with a third-party insurance company, and this was not communicated to the membership by way of adequate privacy disclosure and option to opt out.
➢ Credit union's privacy notice did not align with its current procedures. The notice stated that the credit union shares information with affiliates, but it did not have any affiliates and did not share information in practice.

Source: GAO analysis of examinations with Regulation P violations. | GAO- 21-36

Note: The Consumer Financial Protection Bureau's Regulation P implements the privacy provisions of Title V of the Gramm-Leach-Bliley Act. 15 U.S.C. §§ 6801-6809; 12 C.F.R. pt. 1016.

The regulators with whom we spoke stated that they received few consumer complaints related to financial privacy, and those they did receive were generally minor. Likewise, the regulators observed a few complaints related to financial privacy in institutions' complaint logs. FDIC, the Federal Reserve, OCC, and CFPB review data from their consumer complaint and consumer inquiry programs when monitoring financial institutions or scoping and conducting examinations. NCUA officials told us they received some complaints based on customer misunderstandings and lack of awareness of their opt-out rights and have been working on a customer education program for their members. NCUA has made these concerns a supervisory focus for examinations in 2020.

Federal Prudential Regulators Address Privacy Risks from Third Parties in Their Examinations

In addition to consumer compliance examinations, the prudential regulators (FDIC, Federal Reserve, OCC, and NCUA) further assess how banks and credit unions manage financial privacy risks from third-party relationships as part of their risk-management review for safety and soundness examinations.[56] For example, the prudential regulators told us that they review banks' policies and internal controls and procedures, as well as third-party service agreements, to assess if financial institutions have been taking steps to ensure that third parties with whom they share information comply with various laws, including financial privacy laws.

[56]As discussed later, third parties may be subject to federal oversight because of the relationships into which they have entered with a financial institution.

Regulators conduct these examinations to assess the risk to the regulated institution because the potential failure of the third party to follow such laws could expose the bank or credit union to risk of noncompliance with financial privacy laws.

Federal prudential regulators also have provided guidance to banks and credit unions on ensuring appropriate handling of any nonpublic personal information that third parties hold on the institution's customers. That is, such information must be handled in a manner consistent with the institution's own privacy policy and in accordance with applicable privacy laws and regulations. The guidance explains that financial institutions are expected to conduct proper due diligence in selecting third-party partners and to monitor activities conducted by third parties for compliance with relevant laws, rules, and regulations, considering areas such as consumer protection, security, and privacy requirements.

For example, FDIC, Federal Reserve, and OCC guidance states that banks should adopt risk-management processes that include establishing risk-mitigating controls, retaining appropriate documentation of efforts to obtain information on third parties, and ensuring that contracts meet banks' compliance needs related to financial privacy.[57] Examples of third parties include service providers that deliver products to and perform services on behalf of the institution, such as email marketing vendors or a check printing service. NCUA has similar guidance on third-party risk management for credit unions.[58] Financial institutions and their service providers that maintain, store, or process nonpublic personal information are responsible for that information and its disclosure. Service agreements should address service provider use of nonpublic personal information that was made available to the service provider and direct that the information obtained should be limited to what is needed to provide the contracted services.

[57]Federal Deposit Insurance Corporation, *Guidance for Managing Third-Party Risk,* FIL-44-2008 (Washington, D.C.: June 2008); Board of Governors of the Federal Reserve System, *Guidance on Managing Outsourcing Risk*, SR 13/19/CA 13-21 (Washington, D.C.: December 2013); and Office of the Comptroller of the Currency, *Third-Party Relationships: Risk Management Guidance,* OCC Bulletin 2013-29 (Washington, D.C.: October 2013), as supplemented by *Frequently Asked Questions to Supplement OCC Bulletin 2013-29*, OCC Bulletin 2017-21 (Washington, D.C.: June 2017).

[58]National Credit Union Administration, *Supervisory Letter: Evaluating Third Party Relationships,* SL-07-01 (Washington, D.C.: October 2007).

Safety and soundness examiners from FDIC, Federal Reserve, and OCC told us they do not focus on financial privacy issues because they have not seen elevated risk and concerns based on their preexamination risk assessment for their safety and soundness examinations for the largest banks. For banks with assets of $10 billion or less, privacy is reviewed in their consumer compliance examinations. Examiners from FDIC, Federal Reserve, and OCC, told us that they did not find any significant concerns in banks' third-party risk management as it relates to risk of noncompliance with financial privacy laws and regulations. For depository institutions with assets of over $10 billion, the prudential regulators have signed a memorandum of understanding with CFPB and are required to send copies of all examination reports and material supervision contacts to CFPB and allow the CFPB 30 days to provide any comments or questions. If they find issues related to financial privacy, the issues would be contained within the examination report.

Third-party companies that violate federal consumer financial privacy laws can be subject to enforcement actions by federal agencies. For example, FDIC, the Federal Reserve, and OCC may have enforcement jurisdiction over firms when they are an "institution-affiliated party" under the Federal Deposit Insurance Act or a service company under the Bank Service Company Act. According to NCUA, the agency does not have the same authority as the other prudential regulators over third parties such as service providers and nonaffiliates (as defined by GLBA).

Conclusions

The increasing amounts of and changing ways in which industry collects and shares consumer personal information—including from online activities—highlights the importance of clearly disclosing practices for collection, sharing, and use. However, our work shows that banks and credit unions generally used the model form, which was created more than 10 years ago, to make disclosures required under GLBA. As a result, the disclosures often provided a limited view of how banks and credit unions collect, use, and share personal information. We recognize that the model form is required to be succinct, comprehensible to consumers, and allow for comparability across institutions. But, as information practices continue to change or expand, consumer insights into those practices may become even more limited. Improvements and updates to the model privacy form could help ensure that consumers are better informed about all the ways that banks and credit unions collect, use, and share personal information. For instance, in online versions of privacy notices, there may be opportunities for readers to access additional details—such as through hyperlinks—in a manner consistent with statutory requirements.

Recommendation for Executive Action

The Director of CFPB, in consultation with the other federal financial regulators, should update the model privacy form and, in doing so, consider whether it is feasible to include more comprehensive information about third parties with whom financial institutions share consumer personal information. (Recommendation 1)

Agency Comments and Our Evaluation

We provided a draft of this report to CFPB, FDIC, the Federal Reserve, OCC, and NCUA. We received written comments on the draft from CFPB. In its comments (reprinted in appendix II), CFPB did not state whether it concurred with our recommendation, but said that the agency would consider taking the recommended action, noting that doing so would require a joint rulemaking with other agencies. CFPB also stated that the report provides the public important information about federal oversight of financial institutions' collection, use, and sharing of consumers' personal information and their disclosures to consumers concerning these practices. The Bureau discussed potential approaches to updating the model privacy form and noted that their Trial Disclosure Program Policy allows institutions to make improvements to model forms on a trial basis and may inform CFPB of potential innovations and improvements. As noted in this report, implementing our recommendation will allow consumers to be more informed about the ways that institutions collect, use, and share their personal information. In addition, CFPB noted that updating the model form would not address concerns associated with financial technology applications that aggregate consumer data. We agree that updating the model form will not address these issues. As discussed earlier, we previously made a recommendation to CFPB in a 2018 report to address these issues.[59] FDIC, the Federal Reserve, and OCC also provided technical comments, which we have incorporated in the report, as appropriate. NCUA did not provide any comments.

We are sending copies of this report to the appropriate congressional committees, the Director of CFPB, Chairman of FDIC, Chairman of the Federal Reserve, Chairman of NCUA, Acting Comptroller of the Currency, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

[59]GAO-18-254

If you or your staff have any questions about this report, please contact Alicia Puente Cackley at (202) 512-8678 or CackleyA@gao.gov or Nick Marinos at (202) 512-9342 or MarinosN@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

Sincerely yours,
Alicia Puente Cackley
Director, Financial Markets and Community Investment

Nick Marinos
Director, Information Technology and Cybersecurity

Appendix I: Federal Regulators' Examination Procedures for Assessing Compliance with Financial Privacy Laws

Federal financial regulatory agencies conduct consumer compliance examinations that assess, among other things, a financial institution's policies, procedures, and internal controls for implementing financial privacy laws and regulations.[1] This includes the two examination modules described below, which address certain provisions of the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), and their implementing regulations. These modules cover consumer privacy notices, as well as practices for sharing information with affiliates or with other third parties. Examiners use these modules to review, among other things, for consistency between what institutions tell consumers in notices about their policies and practices and what they actually do.

The Privacy of Consumer Financial Information Examination Procedures guides examiners in assessing if banks and credit unions have been complying with requirements under GLBA and Regulation P to provide privacy notices and restrict disclosure of nonpublic personal information (see fig. 3). If procedural weaknesses or other risks requiring further investigation are found, examiners conduct transaction-level testing.

[1]The federal financial regulatory agencies that examine banks and credit unions for compliance with GLBA are the Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, and National Credit Union Administration.

Figure 3: Key Examination Procedures, Privacy of Consumer Financial Information—Gramm-Leach-Bliley Act

Source: GAO analysis based on examination procedures from federal financial regulators. | GAO-21-36

The FCRA Regulation V Examination Module 2—Obtaining Information and Sharing among Affiliates uses a similarly risk-focused approach to guide examiners in determining a financial institution's compliance with provisions in FCRA and Regulation V that restrict sharing of information among affiliates (and the collection, use, sharing and re-disclosure of a consumer's medical information). Where appropriate, examiners use Module 2 to review bank and credit union policies, procedures, and practices for sharing consumer information with affiliated and nonaffiliated third parties. For example, examiners determine the type of information shared and with whom. If the institution shares information subject to opt-out provisions (such as credit information) with affiliates, examiners also

determine whether the institution's GLBA privacy notice discloses how to opt out in accordance with Regulation V and whether policies and procedures are adequate. Examiners conduct transaction-level testing if procedural weaknesses or other risks requiring further investigation have been noted.

Appendix II: Comments from the Bureau of Consumer Financial Protection

Bureau of Consumer Financial Protection
1700 G Street NW
Washington, D.C. 20552

October 9, 2020

Alicia Puente Cackley
Director
Financial Markets and Community Investment
Government Accountability Office
441 G Street, NW
Washington DC, 20548

Dear Ms. Cackley,

Thank you for the opportunity to review and comment on the draft report by the Government Accountability Office (GAO), titled *Consumer Privacy: Better Disclosures Needed on Information Sharing by Banks and Credit Unions* (21-36). The Consumer Financial Protection Bureau (Bureau) greatly appreciates GAO's work over the course of this engagement and believes the report provides the public important information with regard to Federal oversight of financial institutions' collection, use, and sharing of consumers' personal information and their disclosures to consumers concerning these practices.

Part of the GAO's report focuses on the consumer disclosures required under the privacy provisions of the Gramm-Leach-Bliley Act (GLBA).[1] As noted in the report, the GLBA's privacy provisions generally require that a financial institution provide consumers with notice of the institution's privacy policies and practices and a right to opt-out of the disclosure of consumers' nonpublic personal information to non-affiliated third parties. These provisions also place

[1] 15 U.S.C. §§ 6802–6809. The GLBA's privacy provisions are implemented in the Bureau's Regulation P with respect to financial institutions subject to the Bureau's jurisdiction, 12 C.F.R. pt. 1016, and in rules promulgated by the Federal Trade Commission (FTC), Securities and Exchange Commission (SEC), and Commodity Futures Trading Commission (CFTC) with respect to financial institutions subject to their respective jurisdictions. As noted in the GAO's report, the Bureau does not have authority to supervise for, enforce compliance with, or write regulations implementing the GLBA's data security provisions.

limits on the redisclosure and reuse of consumers' nonpublic personal information and on the sharing of account number information for marketing purposes. The GLBA's privacy provisions were amended in 2006 to require several Federal agencies[2] to jointly develop a model form that may be used, at the option of a financial institution, to provide the required disclosures. The GLBA requires that the model form "be comprehensible to consumers, with a clear format and design; provide for clear and conspicuous disclosures; enable consumers easily to identify the sharing practices of a financial institution and to compare privacy practices among financial institutions; and be succinct and use an easily readable type font."

GAO makes the following recommendation to the Bureau:

- The Director of CFPB, in consultation with the other federal financial regulators, should update the model privacy form and, in doing so, consider whether it is feasible to include more comprehensive information about third-parties with whom financial institutions share consumer personal information.

The Bureau notes that the current model notice was the product of a lengthy effort by multiple agencies and involved extensive consumer testing and several opportunities for public comment.[3] The GAO's report states that the model notice "relies heavily on standardized language, and requires institutions to disclose only a small number of categories of personal information they collect and the ways they use it. As a result, the model form provides consumers with limited insight into the specific information that banks and credit unions collect and who they share it with."[4] As the GAO's report notes, the GLBA requires that the model form be succinct, comprehensible to consumers, and allow comparison among financial institutions.

---

[2] The model notice was adopted pursuant to a joint rulemaking by the Federal banking agencies (the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision), the National Credit Union Administration, the SEC, the CFTC, and the FTC.

[3] The Supplementary Information to the Notice of Proposed Rulemaking for the model notice and final rule contains a detailed discussion of (1) consumer research on the development and testing of the model notice; (2) public comments received on an Advance Notice of Proposed Rulemaking relating to improving GLBA privacy notices, a Notice of Proposed Rulemaking proposing the model notice, and the publication of experts' reports and consumer testing data relating to the model notice; and (3) other stakeholder engagement concerning improvements to GLBA privacy notices. 72 Fed. Reg. 14940, 14942–44 (March 29, 2007); 74 Fed. Reg. 62890 (Dec. 1, 2009).

[4] GAO, *Consumer Privacy: Better Disclosures Needed on Information Sharing by Banks and Credit Unions*, GAO-21-36 (Draft September 2020), at 19.

The model notice reflects the agencies' determination that standardization enables consumers to compare privacy practices across institutions and that the inclusion of greater volumes of information about a financial institution's practices would generally defeat the goal of making the notice more understandable to consumers.[5] We also note that the GLBA requires that financial institutions disclose the *categories* of persons to whom consumer information is or may be disclosed.

The GAO's report also suggests that increases in data sharing practices since the model form was adopted in 2009 support updating the model notice. The report notes increased consumer use of "fintech" applications, which rely on a consumer's authorization to access financial data in order to provide products and services to the consumer, and states that consumers may be largely unaware of how these applications collect, use, and share their information. It is not entirely clear, however, how GAO believes the model form should be revised to increase consumer understanding in this area. For example, where data sharing is consumer-authorized, the consumer is already aware that the data held by its bank or credit union will be shared with the authorized third party. Third parties accessing consumer data pursuant to consumer authorization that are themselves financial institutions subject to Regulation P would be required to provide disclosures that satisfy Regulation P's requirements, such as the model notice. The Bureau's authority under the GLBA, however, could not be used to require disclosures by entities that are not financial institutions subject to the GLBA.

Nonetheless, the Bureau has been very engaged in the area of consumer-authorized data access and, to date, has sought to identify and promote consumer interests in this area, including those relating to consumer control, privacy, and data security, while allowing the market to develop

[5] The agencies noted soon after the GLBA privacy notice requirements went into effect that many notices provided to consumers were long and complex, and were formatted in various ways, making them difficult for consumers to compare, even among financial institutions with identical practices. *See, e.g.*, 72 Fed. Reg. at 14943; 74 Fed. Reg. at 62893. In adopting the final rule, the agencies noted that, "[b]ased on the statutory requirement that the Agencies propose a 'model form', the final model privacy form utilizes a standardized format. Moreover . . . the Agencies research supports uniform disclosures to help consumers better understand companies' information sharing practices." 74 Fed. Reg. at 62897. In response to industry commenters that proposed terms used in the model notice table to describe sharing practices were abbreviated and incomplete, the agencies concluded that, if they were to "add to the laundry list of descriptive terms to make the provisions in the table more 'precise,'" it would "defeat the purposes of making this information more understandable to consumers." 74 Fed. Reg. at 62903.

without direct regulatory intervention.[6] As the report notes, the Bureau recently announced that it intends to issue an advance notice of proposed rulemaking (ANPR) later this year to request feedback on how it might implement Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act), which provides for consumer access to financial records. In this ANPR, the Bureau intends to seek comment on various topics relating to consumer-authorized data access by third parties such as fintech applications, including the extent of consumer understanding of these parties' data collection, use, and sharing practices, and the sufficiency of consumer disclosures by these parties concerning such practices.

We note that the Bureau's Trial Disclosure Program Policy (TDP Policy) provides an opportunity for covered persons to innovate improvements to the Regulation P model notice pursuant to a trial disclosure program.[7] The Dodd-Frank Act provides that the Bureau may permit covered persons to conduct trial disclosure programs, limited in time and scope, for the purpose of testing disclosures designed to improve upon model forms within the Bureau's jurisdiction.[8] For permitted trial disclosure programs, the Bureau expects to deem the applicant to be in compliance with, or exempt from, described Federal disclosure requirements, for a limited period of time.[9] As noted in the TDP Policy, the Bureau believes that there may be significant opportunities to enhance consumer protection by facilitating innovation through enabling responsible companies to research informative, cost-effective disclosures in test programs. The Bureau also recognizes that in-market testing may offer particularly valuable information with which to improve disclosure rules and model forms. We note that, pursuant to the TDP Policy, trial disclosure programs may be facilitated by trade associations, consumers groups, or other third parties that are not themselves covered persons.[10]

---

[6] For example, in 2017, the Bureau issued "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation," which covered nine topics related to consumer-authorized access: access; data scope and usability; control and informed consent; authorizing payments; security; access transparency; accuracy; ability to dispute and resolve unauthorized access; and efficient and effective accountability mechanisms. Consumer Financial Protection Bureau, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* (October 2017), available at *https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf*.

[7] 84 Fed. Reg. 48260 (Sept. 13, 2019).

[8] 12 U.S.C. § 5532(e)(1).

[9] 84 Fed. Reg. at 48268.

[10] 84 Fed. Reg. at 48271.

The Bureau is committed to ensuring that financial institutions' disclosures to consumers accomplish their consumer protection and transparency goals and will consider the GAO's recommendation. We note that updating the model privacy form would likely involve a joint rulemaking between the Bureau, the SEC, the CFTC, and the FTC. If the Bureau determines a rulemaking is warranted, its process for setting its rulemaking agenda considers various factors, including risks to consumers, the benefits to consumers and costs to industry of possible regulatory interventions, the relevant statutory framework, and available resources. While revising the model privacy form is not currently on the Bureau's rulemaking agenda, the Bureau will continue to monitor developments in this area, including any possible improvements to the model form identified pursuant to the Bureau's TDP Policy. Together with other regulators, it will consider whether a rulemaking might be appropriate or warranted in the future.

Sincerely,

Kathleen L. Kraninger
Director

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Alicia Puente Cackley, (202) 512-8678, CackleyA@gao.gov

Nick Marinos, (202) 512-9342, MarinosN@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Kay Kuhlman (Assistant Director, FMCI), John de Ferrari (Assistant Director, ITC), Kavita Daitnarayan (Analyst in Charge), Jill Lacey, Kirsten Noethen, Akiko Ohnuma, Barbara Roesmann, Richard Sayoc, and Jena Sinkfield made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548