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.