September 2014

CONSUMER FINANCIAL PROTECTION BUREAU

Some Privacy and Security Procedures for Data Collections Should Continue Being Enhanced

GAO Highlights

Highlights of GAO-14-758, a report to congressional addressees

Why GAO Did This Study

Congress created CFPB in 2010 as an independent agency to regulate the provision of consumer financial products and services, such as mortgages and student loans. CFPB has begun collecting consumer financial data from banks, credit unions, payday lenders, and other institutions. GAO was mandated to examine CFPB's collection of consumer financial data. This report addresses (1) the scope, purposes, uses, and authorities of CFPB consumer financial data collections and (2) CFPB's compliance with laws and federal requirements, including government-wide privacy and information security requirements.

GAO reviewed laws, regulations, and contracts pertaining to CFPB's data collections; reviewed privacy and information security policies; reviewed inspector general reports on CFPB's information security program; assessed how CFPB applied NIST's framework for managing risks of storing data; examined access controls on the system maintaining consumer financial data; and interviewed CFPB and other regulatory officials, privacy experts, and representatives from randomly selected financial institutions.

What GAO Recommends

GAO makes 11 recommendations to enhance CFPB's privacy and information security and 1 recommendation to OCC to ensure its data collections comply with appropriate disclosure requirements. CFPB and OCC agreed with GAO's recommendations and noted steps they plan to take or have taken to address them.

View GAO-14-758. For more information, contact A. Nicole Clowers, 202-512-8678, clowersa@gao.gov.

What GAO Found

To carry out its statutory responsibilities, the Consumer Financial Protection Bureau (CFPB) has collected consumer financial data on credit card accounts, mortgage loans, and other products through one-time or ongoing collections. As the following table shows, these large-scale data collections varied from about 11,000 consumer arbitration case records from a trade association to 173 million mortgage loans from a data aggregator. Of the 12 large-scale collections GAO reviewed, 3 included information that identified individual consumers, but CFPB staff indicated that those 3 were not subject to statutory restrictions on collecting such information. Other regulators, such as the Board of Governors of the Federal Reserve System (Federal Reserve) and the Office of the Comptroller of the Currency (OCC), collect similarly large amounts of data.

CFPB has taken steps to protect and secure these data collections. For example, it created a data intake process that brings together staff with relevant expertise to consider the statutory, privacy, and information security implications of proposed consumer financial data collections. CFPB staff described a process for anonymizing large-scale data collections that directly identify individuals. In addition, CFPB had taken steps to implement an information security program that is consistent with Federal Information Security Management Act requirements, according to the Office of Inspector General for the Federal Reserve and CFPB. GAO found that CFPB had implemented logical access controls for the information system that maintains the consumer financial data collections and was appropriately scanning for problems or vulnerabilities. CFPB also established a risk-management process for the information system that maintains consumer financial data consistent with guidelines developed by the National Institute of Standards and Technology (NIST).

However, GAO determined that additional efforts are needed in several areas to reduce the risk of improper collection, use, or release of consumer financial data.

- **Written procedures and documentation:** CFPB lacks written procedures and comprehensive documentation for a number of processes, including data intake and information security risk assessments. The lack of written procedures could result in inconsistent application of the established practices. For example, CFPB unnecessarily retained sensitive data in two collections GAO reviewed, but its staff said they plan to remove this information. GAO recommends CFPB establish or enhance written procedures for (1) data intake, including reviews of proposed data collections for compliance with applicable legal requirements and restrictions; (2) anonymizing data; (3) assessing and managing privacy risks; and (4) monitoring and auditing privacy controls; and (5) documenting results of information security risk-assessments consistently and comprehensively.
- **Implementation of privacy and security steps:** CFPB has not yet fully implemented a number of privacy control steps and information security practices, which could hamper the agency's ability to identify and monitor privacy risks and protect consumer financial data. GAO recommends CFPB take or complete action to (1) develop a comprehensive written privacy plan that brings together existing privacy policies and guidance; (2) obtain periodic

independent reviews of its privacy practices; (3) develop and implement targeted privacy training for staff responsible for working with sensitive personal information; (4) update remedial action plans to include all identified weaknesses and realistic planned remediation dates that reflect priorities and resources; and (5) include an evaluation of compliance with contract provisions relating to information security in CFPB's review of the service provider that processes consumer financial data on its behalf.

- **Paperwork Reduction Act compliance:** Under the Paperwork Reduction Act (PRA), agencies generally must obtain Office of Management and Budget (OMB) approval when collecting data from 10 or more entities to minimize burden and maximize the practical utility of the information collected. CFPB and OCC collect, on an ongoing basis, credit card data from different institutions—representing about 87 percent of outstanding credit card balances—and agreed to share data. However, OMB staff said the agencies' collections and data-sharing agreement may warrant OMB review and approval. Additional consultation with OMB regarding these collections and the data-sharing agreement would help both agencies ensure they are fully complying with the law. Furthermore, OCC had not obtained OMB approval for its credit card and mortgage data collections, which each included more than nine entities. Without approval, OCC lacks reasonable assurance that its collections comply with PRA requirements intended to reduce burden. GAO recommends (1) CFPB consult further with OMB about its credit card collection and data-sharing agreement, and (2) OCC seek OMB approval for its credit card and mortgage data collections.

CFPB's Large-Scale Collections of Consumer Financial Data from January 2012 through July 1, 2014

Data collection	Scope	Ongoing or one-time	Contains information that directly identifies individuals?
Arbitration case records: consumer case records from January 2010 through early 2013	11,204 case records	One-time	✓
Automobile sales: vehicle transaction-level data from 46 state motor vehicle departments matched with consumer credit data	700,000 vehicles per month	Ongoing (monthly)	
Consumer credit report information: nationally representative sample panel of consumer credit information	10.7 million individuals	Ongoing (monthly and quarterly)	
Credit cards: individual consumers' credit card account-level data, with linkages to credit reporting data	25-75 million total accounts[a]	Ongoing (monthly)	
Credit scores: random samples of consumer reports and credit scores calculated on such reports	600,000 consumer credit reports	One-time	
Deposit advance products: deposit account and transaction-level data, including use of deposit advance products	100,000-500,000 accounts	One-time	✓[b]
Mortgages: loan-level data from large servicers for mortgages	29 million active loans; 173 million total loans	Ongoing (monthly)	
Online payday loans: loan summaries from a sample of borrower files from online payday lenders, matched with consumer credit data	300,000 borrowers	One-time	
Overdraft fees: account and transaction-level data based on random samples of consumer checking accounts	2 million accounts and related transactions	One-time	
Private-label mortgages: loan-level data on loans packaged into private-label mortgage-backed securities	4 million active loans; 21.9 million total loans	Ongoing (monthly)	
Private student loans: loan-level data on all educational loan originations from 2005 through 2011	5.5 million total loans	One-time	
Storefront payday loans: borrower-level activity for all loans within a period of 12 or more months	15-40 million total loans	One-time	✓[b]

Source: GAO analysis of CFPB information. | GAO-14-758

[a]CFPB has access to credit card data from additional credit card issuers through an information-sharing agreement with the Office of the Comptroller of the Currency, which collects more than 500 million total accounts on a monthly basis. When combined, these data contain information about 87 percent of outstanding credit card balances by volume as of March 2014.

[b]CFPB removed information that directly identifies individuals from the files staff use to analyze these data.