Congressional Research Service
Informing the legislative debate since 1914

The Equifax Data Breach: An Overview and Issues for Congress

September 29, 2017

According to Equifax, cybercriminals exploited a vulnerability in one of its online applications between mid-May and July 2017, potentially revealing information for 143 million U.S. consumers. Equifax stated that "the information accessed primarily includes names, Social Security numbers, birth date, addresses, and, in some cases, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed." Much of the information that Equifax listed is difficult or impossible to change, potentially exposing affected individuals to significant risk of identity theft in the future.

Credit Reporting Agencies

Equifax is a credit reporting agency (CRA). CRAs collect information to develop credit reports about individuals. A credit report typically includes information related to a consumer's identity (such as name, address, and Social Security number), existing or recent credit transactions (including credit card accounts, mortgages, and other forms of credit), public record information (such as court judgments, tax liens, or bankruptcies), and credit inquiries made about the consumer.

The three largest CRAs—Equifax, TransUnion, and Experian—are the most well-known, but they are not the only CRAs. Approximately 400 smaller CRAs either are regional or specialize in collecting specific types of information or for specific industries, such as information related to payday loans, checking accounts, or utilities.

Credit reports are used in several ways. Lenders use credit reports to evaluate loan applications. Landlords may use credit information to help to decide whether to rent to a household. Some employers use credit reports to evaluate job applicants. Insurance companies use customized credit reports with claims histories to set rates.

Regulation of Credit Reporting Agencies

CRAs are subject to many different laws and regulations related to nearly all aspects of their business. Much of what is thought of as the business of credit reporting is regulated through the Fair Credit Reporting Act (FCRA). The FCRA requires "that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information." The FCRA establishes consumers' rights

in relation to their credit reports, as well as permissible uses of credit reports. It also imposes certain responsibilities on those who collect, furnish, and use the information contained in consumers' credit reports.

Although originally the FCRA delegated rulemaking and enforcement authority to the Federal Trade Commission (FTC), the Dodd-Frank Act transferred that authority to the Consumer Finance Protection Bureau (CFPB). The CFPB coordinates enforcement efforts with the FTC's enforcements under the Federal Trade Commission Act. Since 2012, the CFPB has subjected the "larger participants" in the consumer reporting market to supervision. Previously, CRAs were not actively supervised for FCRA compliance on an ongoing basis.

CRAs are subject to the data protection requirements of Section 501(b) of the Gramm-Leach-Bliley Act (GLBA). Section 501(b) requires the federal financial institution regulators to "establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguard—(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access or use of such records or information which could result in substantial harm or inconvenience to any customer."

As the "federal functional regulator" of CRAs and other nonbank financial institutions, the FTC has promulgated 15 C.F.R. §341 implementing this requirement and subjecting CRAs to its provisions. The FTC has authority, under GLBA, to enforce this regulation with respect to the CRAs through its authority under the Federal Trade Commission Act. The FTC, however, has little up-front supervisory or enforcement authority, making it difficult to prevent an incident from occurring and instead often relying on enforcement after the fact. As mentioned above, the CFPB does have supervisory authority over the CRAs, but that authority appears to be limited. The CFPB has asserted that Dodd-Frank "excluded financial institutions' information security safeguards under GLBA Section 501(b) from the CFPB's rulemaking, examination, and enforcement authority."

Potential Issues for Congress

Many Members have expressed significant concerns about the Equifax breach, and at least four committees have announced hearings to examine the breach more closely. Several issues are likely to be of interest during the hearings and subsequent policy debate.

Data Breach. The announcement by Equifax has left a significant amount of uncertainty related to the breach itself. When Equifax stated that information was "accessed," it is unclear if that means the consumer data was observed using the unauthorized access or if data was downloaded by an unauthorized party. The data breach has also raised questions about whether Equifax's safeguards were in compliance with GLBA and other data protection requirements.

Legal Framework. The incident has prompted some to question whether the regulatory framework for CRAs is appropriate. The FCRA contains certain consumer protections, but some have called for additional safeguards, such as allowing consumers to freeze their credit report for free or to opt out of having their information collected. Others have called for more stringent data protection requirements and a uniform nationwide data breach notification law to replace state laws so that all consumers would be notified in a timely manner if their data is compromised. Congress may also reassess whether the CFPB, which has supervisory authority over CRAs that are larger participants, should have explicit supervisory authority over cybersecurity at CRAs.

Regulatory Response. Multiple agencies are reportedly investigating the breach. The breach also raises questions about the performance of Equifax's regulators and whether any action on their part could have prevented the incident. The director of the CFPB recently stated during an interview that the CFPB would

be changing its supervisory regime for the three largest CRAs and that the CRAs were "going to have monitoring in place that's preventive." It is unclear what the enhanced monitoring would look like and whether it would have been able to prevent the Equifax incident.

Author Information

N. Eric Weiss
Specialist in Financial Economics

Disclaimer