

GAO Highlights

Highlights of [GAO-18-559](#), a report to congressional requesters.

Why GAO Did This Study

CRA's such as Equifax assemble information about consumers to produce credit reports and may provide other services, such as identity verification to federal agencies and other organizations. Data breaches at Equifax and other large organizations have highlighted the need to better protect sensitive personal information.

GAO was asked to report on the major breach that occurred at Equifax in 2017. This report (1) summarizes the events regarding the breach and the steps taken by Equifax to assess, respond to, and recover from the incident and (2) describes actions by federal agencies to respond to the breach. To do so, GAO reviewed documents from Equifax and its cybersecurity consultant related to the breach and visited the Equifax data center in Alpharetta, Georgia, to interview officials and observe physical security measures. GAO also reviewed relevant public statements filed by Equifax. Further, GAO analyzed documents from the IRS, SSA, and USPS, which are Equifax's largest federal customers for identity-proofing services, and interviewed federal officials related to their oversight activities and response to the breach.

What GAO Recommends

GAO is not making recommendations in this report. GAO plans to issue separate reports on federal oversight of CRA's and consumer rights regarding the protection of personally identifiable information collected by such entities. A number of federal agencies and Equifax provided technical comments which we incorporated as appropriate.

View [GAO-18-559](#). For more information, contact Nick Marinos at (202) 512-9342 or MarinosN@gao.gov, or Michael Clements at (202) 512-8678 or ClementsM@gao.gov.

DATA PROTECTION

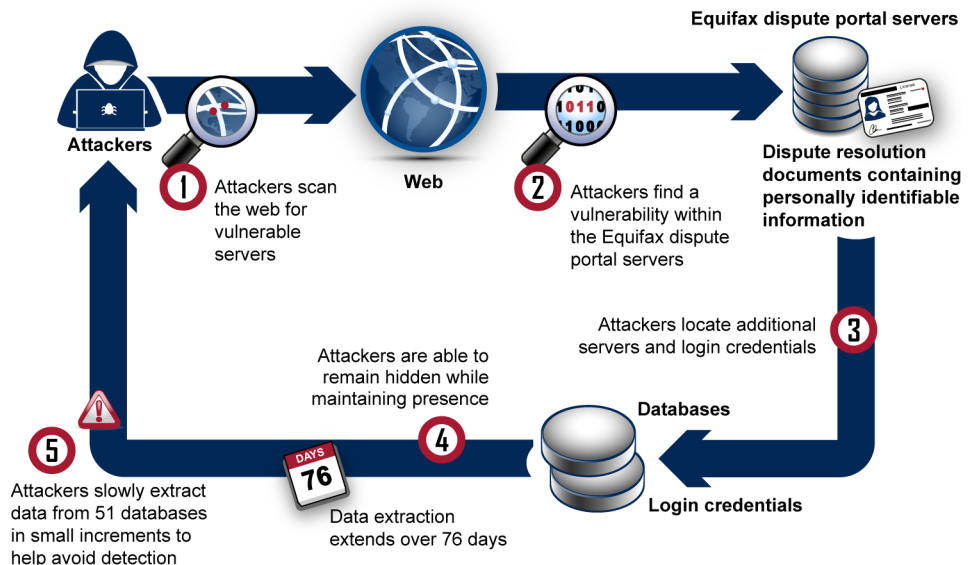
Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach

What GAO Found

In July 2017, Equifax system administrators discovered that attackers had gained unauthorized access via the Internet to the online dispute portal that maintained documents used to resolve consumer disputes (see fig.). The Equifax breach resulted in the attackers accessing personal information of at least 145.5 million individuals. Equifax's investigation of the breach identified four major factors including identification, detection, segmenting of access to databases, and data governance that allowed the attacker to successfully gain access to its network and extract information from databases containing personally identifiable information. Equifax reported that it took steps to mitigate these factors and attempted to identify and notify individuals whose information was accessed. The company's public filings since the breach occurred reiterate that the company took steps to improve security and notify affected individuals.

The Internal Revenue Service (IRS), Social Security Administration (SSA), and U.S. Postal Service (USPS)—three of the major federal customer agencies that use Equifax's identity verification services—conducted assessments of the company's security controls, which identified a number of lower-level technical concerns that Equifax was directed to address. The agencies also made adjustments to their contracts with Equifax, such as modifying notification requirements for future data breaches. In the case of IRS, one of its contracts with Equifax was terminated. The Department of Homeland Security offered assistance in responding to the breach; however, Equifax reportedly declined the assistance because it had already retained professional services from an external cybersecurity consultant. In addition, the Bureau of Consumer Financial Protection and the Federal Trade Commission, which have regulatory and enforcement authority over consumer reporting agencies (CRA's) such as Equifax, initiated an investigation into the breach and Equifax's response in September 2017. The investigation is ongoing.

How Attackers Exploited Vulnerabilities in the 2017 Breach, Based on Equifax Information



Source: GAO, based on information provided by Equifax. | GAO-18-559