CRS INSIGHT

The Yahoo! Data Breach—Issues for Congress

September 26, 2016 (IN10586)

|

Related Author

- N. Eric Weiss

|

N. Eric Weiss, Specialist in Financial Economics (eweiss@crs.loc.gov, 7-6209)

On September 22, 2016, Yahoo! announced that information on at least 500 million user accounts had been stolen. It reported that compromised information included "names, email addresses, telephone numbers, dates of birth, hashed passwords ... and, in some cases, encrypted or unencrypted security questions and answers." The breach started in late 2014, but Yahoo! did not say when it was detected.

It is not clear what the impact on individuals will be. It appears that passwords were properly secured, but if a state actor with immense resources is involved, the passwords could be compromised. Since passwords frequently are used on several websites, other accounts could be at risk. A malicious actor might be able to use the security questions for personalized phishing attacks.

Yahoo! has released very limited information about the data breach. For example, it has not announced how many of the 500 million leaked email addresses were for people in the United States (population 325 million), and it has not said how many individuals have multiple accounts. The size of the breach suggests that regulators in Europe and Asia may become involved.

The breach could have a financial impact on Yahoo!. There will be the cost of investigations and remediation. In July 2016, Verizon agreed to purchase Yahoo! for $4.6 billion. The breach could affect the merger in several ways, including a delay while the investigation continues; the terms of the merger could be changed; or the merger could be cancelled.

A large data breach, such as this one, raises three sets of issues for Congress: (1) should there be a federal notification requirement, (2) do federal agencies (i.e., the Federal Trade Commission [FTC]) have adequate authority to protect consumers, and (3) should there be federal data security standards?

Data Breach Notification Laws

Currently, federal law requires only a few specific sectors to notify consumers of a data breach. These include certain financial institutions covered by the Gramm-Leach-Bliley Act and certain health care entities covered by the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act.

Bills have been introduced in the 114th and earlier Congresses that would create a federal data breach consumer

notification requirement. Business groups representing the financial and retail sectors, such as the Financial Services Roundtable and the National Retail Federation, have recently called for passage of a federal data breach notification law. One key issue is whether the federal law would preempt state laws and prevent states from mandating stricter notification standards. Currently, 47 states and the District of Columbia have data breach notification laws.

In general, state data breach notification laws define covered entities, covered information, what constitutes a covered data breach, how and when notice must be delivered, penalties and enforcement authorities, and remedies for those harmed does it create. There are many definitions of what comprises "personally identifiable information" (PII). GAO has defined it as "any information that can be used to distinguish or trace an individual's identity such as name ... date and place of birth." Thus it seems that the Yahoo! leak includes PII regardless of what PII might be contained in the security questions. This might trigger certain state data breach notification laws.

Modifying Federal Trade Commission Statutory Powers

Currently, the FTC relies on its broad statutory authority under Section 5 of the Federal Trade Commission Act (15 U.S.C. §45) to pursue data security violations. First, if a company makes materially misleading statements or omissions relating to its data security practices and such statements or omissions are likely to mislead reasonable consumers, the FTC has argued that a company has engaged in unfair and deceptive practices prohibited by Section 5. The company can agree with the FTC, negotiate a consent agreement with the FTC, or deny the FTC's claim. In this latter situation, the FTC could sue the company, alleging they engaged in unfair and deceptive practices prohibited under Section 5. Second, the FTC has argued that if a company's data security practices either "cause or are likely to cause substantial injury to consumers that is not reasonably avoidable by consumers nor are outweighed by benefits to consumers or to competition," those practices can be found to violate Section 5.

Some in Congress have called for passage of a law to strengthen the FTC's statutory authority to penalize businesses that fail to adequately protect consumers' personally identifiable information.

Creating Federal Standards for Data Security, Including for Businesses

Some contend that a federal data breach notification law on its own would not combat widespread data breaches, primarily because the notification comes after the fact of a breach. These critics advocate that in addition to data breach notification, the federal government should create standards for what represents a minimum acceptable level of data security. One study noted that a lack of clarity in terms of what precautions businesses should take to protect consumers' personal information has resulted in a patchwork of state data security standards. Although the FTC has proposed some generic guidelines, the agency arguably does not have authority to promulgate official regulations, which could detail such standards more fully.

Creating a federal standard for data security has both proponents and opponents in Congress. On the one hand, critics voice concerns that a federal standard would be too rigid for such a rapidly evolving, technology-driven field as data security. They fear that a federal standard could be burdensome and could lag behind new technological trends or discourage businesses from adopting newer technologies to prevent fraud. On the other hand, proponents of creating federal data security standards argue that such a standard need not be specific nor advocate particular technologies. According to this argument, the federal statute could, for example, consist of a mandate that an organization employ a level of data security that reflects the size and complexity of its data operations, for the cost of available tools to reduce vulnerabilities, and for the volume and sensitivity of consumer information it holds.