AG Settlements Call for Stronger Data Security

Paul L. Singer, Beth Bolen Chun

November 10, 2022

Early this week, a coalition of 40 attorneys general obtained two multistate settlements with Experian concerning data breaches it experienced in 2012 and 2015 that compromised the personal information of millions of consumers nationwide. The 2012 breach investigation was co-led by the Massachusetts and Illinois AG offices, and the 2015 investigation was co-led by the AGs of Connecticut, DC, Illinois, and Maryland. An additional settlement was reached with T-Mobile in connection with the 2015 Experian breach, which impacted more than 15 million individuals who submitted credit applications with T-Mobile.

In an effort to change corporate behavior, both settlements require Experian and T-Mobile to enhance their data security practices and to pay a combined amount of more than $16 million. Experian has agreed to bolster its due diligence and data security practices by adhering to the following:

- prohibition against misrepresentations to its clients regarding the extent to which Experian protects the privacy and security of personal information;
- implementation of a comprehensive Information Security Program,
- incorporating zero-trust principles, regular executive-level reporting, and enhanced employee training;
- due diligence provisions requiring the company to properly vet acquisitions and evaluate data security concerns prior to integration;
- data minimization and disposal requirements, including specific efforts aimed at reducing use of Social Security numbers as identifiers; and
- specific security requirements, including with respect to encryption, segmentation, patch management, intrusion detection, firewalls, access controls, logging and monitoring, penetration testing, and risk assessments.

T-Mobile has agreed to bolster its vendor oversight moving forward, including:

- implementation of a Vendor Risk Management Program;
- maintenance of a T-Mobile vendor contract inventory, including vendor criticality ratings based on the nature and type of information that the vendor receives or maintains;
- imposition of contractual data security requirements on T-Mobile’s vendors and sub-vendors, including related to segmentation, passwords, encryption keys, and patching;

- establishment of vendor assessment and monitoring mechanisms; and
- taking appropriate action in response to vendor non-compliance, up to contract termination.

Note that the settlement with T-Mobile doesn't concern the unrelated data breach announced by T-Mobile in August 2021, which is currently under investigation by a collection of states.

Alongside the 2015 data breach settlements, Experian has agreed to pay an additional $1 million to resolve an independent multistate investigation into another Experian-owned company—Experian Data Corp. (“EDC”). Such investigation was in connection with EDC’s failure to prevent or provide notice of a 2012 data breach initiated by an identity thief posing as a private investigator who was given access to sensitive personal information stored in EDC’s commercial databases. As a result, EDC has agreed to strengthen its vetting and oversight of third parties to which it provides personal information, investigate and report data security incidents to the Attorneys General, and maintain a “Red Flags” program to detect and respond to prospective identity theft.

Although every state has a breach notification law that generally gives rise to these types of enforcement actions, companies may wonder at times what a particular State considers to be reasonable data security practices to avoid potential liability. Whether you are a CEO or privacy manager, States expect that privacy and data security awareness is interwoven into the fabric of a business’s culture. Reviewing the injunctive terms achieved in these settlements and others can be instructive in understanding AG expectations for data security practices and managing risk.