



BRIAN E. FROSH, MARYLAND ATTORNEY GENERAL

PRESS RELEASE

FOR IMMEDIATE RELEASE

Media Contacts:
press@oag.state.md.us
410-576-7009

Attorney General Frosh Enters into Multistate Settlements Addressing 2015 Experian Data Breach

***Experian Information Solutions, Inc. and T-Mobile USA, Inc. Agree to Pay
More than \$15 Million and Improve Their Data Security Practices***

BALTIMORE, MD (November 7, 2022) – Maryland Attorney General Brian E. Frosh today announced separate settlements with Experian Information Solutions, Inc. (Experian) and T-Mobile USA, Inc. (T-Mobile) concerning a 2015 data breach experienced by Experian that compromised the personal information of more than 15 million individuals who submitted credit applications with T-Mobile. The settlements were negotiated by a multistate work group that included 40 states and was led by the Maryland Attorney General’s Office. Under the settlements, the companies have agreed to improve their data security practices and to pay the states a combined amount of more than \$15 million. The personal information of at least 376,170 Marylanders was compromised by the breach.

“The 2015 data breach of Experian’s network exposed millions of individuals to the risk of identity and financial theft,” said Attorney General Frosh. “Consumers put their trust in T-Mobile and Experian when they provided personal information to apply for T-Mobile’s services. What they got instead is the risk that they may become victims of identity theft.”

In September 2015, Experian, one of the big-three credit reporting bureaus, reported it had experienced a data breach in which an unauthorized actor gained access to part of Experian’s network storing personal information on behalf of its client, T-Mobile. The breach involved information associated with consumers who had applied for T-Mobile’s postpaid services and device financing between September 2013 and September 2015, including names, addresses, dates of birth, Social Security numbers, identification numbers (such as driver’s license numbers and passport numbers), and related information used in T-Mobile’s own credit assessments. Neither Experian’s consumer credit database, nor T-Mobile’s own systems, were compromised in the breach.

The multistate coalition obtained separate settlements from [Experian](#) and [T-Mobile](#) in connection with the 2015 data breach. Under a \$12.67 million settlement, Experian has agreed to strengthen its due diligence and data security practices going forward, including:

- 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.

The settlement also requires Experian to offer five years of free credit monitoring services to affected consumers, as well as two free copies of their credit reports annually during that timeframe. This is in addition to the four years of credit monitoring services that had already been offered to affected consumers – two of which were offered by Experian in the wake of the breach, and two that were secured through a separate 2019 class action settlement. Enrollment in these prior offerings is now closed.

Consumers, including those covered by the 2019 class action settlement, can enroll in the 5-year extended credit monitoring services. More information on eligibility can be found at www.tmobileapplicant2015eisdatabreachsettlement.com.

In a separate \$2.43 million settlement, T-Mobile has agreed to detailed vendor management provisions designed to strengthen its vendor oversight going 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
- Appropriate action in response to vendor non-compliance, up to contract termination.

The settlement with T-Mobile does not concern the unrelated data breach announced by T-Mobile in August 2021.

Along with Maryland, the investigation into the 2015 data breach was co-led by Connecticut, the District of Columbia, and Illinois, with the assistance of Massachusetts and Texas. The settlement was also joined by Arizona, Arkansas, Delaware, Florida, Georgia, Hawaii, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, Tennessee, Vermont, Virginia, Washington, and Wisconsin.

Consumers with concerns about identity theft may contact the Attorney General’s Identity Theft Unit by calling 410-576-6491 or email to IDTheft@oag.state.md.us.

<https://www.marylandattorneygeneral.gov/press/2022/110722a.pdf>