



# Security Breach at Experian Exposes Personal Data of 15 Million T-Mobile Customers and Prospective Customers

Insights

10.02.15

On October 1, 2015, Experian, the world's largest consumer credit monitoring firm, announced that an unauthorized party (i.e., hacker) had gained access to the personal data of approximately 15 million customers and prospective customers of its client, T-Mobile, which data was housed on an Experian network server. The exposed records included information such as the consumer's name, address, Social Security number, date of birth, identification number (e.g., driver's license, military ID or passport number) and additional information which T-Mobile uses in its own credit assessment, such as consumer payment history. The breach did not include payment card or banking information. The consumers impacted were those who had applied for services with T-Mobile between September 1, 2013 and September 16, 2015, many of whom were new applicants on whom Experian was performing a credit check for service or device financing. Experian was encrypting stored Social Security numbers and identity numbers, but told T-Mobile that it believed the hacker had cracked the encryption.

According to a Q&A posted on its website, Experian first discovered the breach on September 15<sup>th</sup>, but indicates that its "first priority was mitigation and containment, followed by conducting an investigation" – in order to validate that it had successfully contained the breach and determined its scope – after which it began notifying impacted individuals. Some of the steps Experian took to mitigate the problem included assessing and removing malware or improper connectivity, performing assessment of isolation procedures of the affected server and associated systems and increasing monitoring. Experian is offering to all affected individuals two years of free credit monitoring and identity resolution services through Experian's own ProtectMyID service. The service provides participants with a credit report upon enrollment, credit monitoring from all three nationwide credit reporting agencies, internet scans and access to specialized fraud resolution agents. Still, some impacted individuals have questioned whether the company who was hacked should be the one doing the monitoring.

T-Mobile's Chief Executive Officer, John Legere, has said he is "incredibly angry" about the breach and that T-Mobile will be conducting a thorough review of its relationship with Experian. Experian says that it has notified law enforcement in the U.S. and abroad. The Connecticut Attorney General's Office said it would investigate this recent attack, and confirmed that its investigation of an earlier data breach at Experian subsidiary Court Ventures in 2012, where a Vietnamese fraudster was able

to purchase personal information relating to 200 million people which he then sold to cybercriminals, was still under investigation.