For Sale: $10 for 10 records— Records from the T-Mobile hack surface for sale on the dark net

DATA PRIVACY SOLUTIONS | OCT 08, 2015

Another day— another data breach. Last week, T-Mobile announced that the company it partnered with to run credit checks had suffered a security breach, which allowed hackers access to sensitive data of 15 million T-Mobile credit applicants. The exposed information included the names, addresses, birthdays, and encrypted Social Security numbers and/or encrypted driver's license or passport numbers of approximately 15 million people who applied for T-Mobile services between September 1, 2013 and September 16, 2015. While encryption was used, it appears to have been compromised, though the hackers were not able to steal bank account or credit card information.

This case is somewhat similar to the 2012 Target breach where the hackers infiltrated one of Target's HVAC vendors and got into Target's POS system from the third-party vendor's access to Target's network. Here, the hackers infiltrated T-Mobile's partner, which had T-Mobile's credit card applicant information.

While the partner company has taken full responsibility for the theft from its server, there are still major reputational and legal hurdles facing T-Mobile. As such, the next logical question is, how did the partner company get all this information that belonged to T-Mobile? As it turns out, like many other companies, T-Mobile uses the partnering entity to store personal information for applicants as the partner entity determines whether an applicant will be approved for credit. It certainly makes sense seeing as how the partner entity is one of the top three credit scoring companies. The law requires the partner entity to keep credit application data for 25 months.

Black Market

Those affected have been offered two years of credit monitoring services from ProtectMyId, and it looks like they will need it because there have already been reports that the compromised information is now for sale on the Internet's black market. One cybersecurity firm reported that a number of new listings surfaced on the dark net, which includes advertising information matching the type of T-Mobile payment information that was exfiltrated from the partner entity. Listings for FULLZ data, a reference to someone who has been hacked, were posted throughout the dark net the day after T-Mobile reported the breach. One ad offers 10 records for $10 ($1 per record) payable in Bitcoin. While it is certainly possible the listings are fake, they are still out there and only time will tell if they are real. So far, there has not been any indication that the stolen customer information has been used. The scope of the fall-out and the total damage remain to be seen.

From T-Mobile's perspective, they have various concerns. The first is certainly protecting the privacy of their credit card applicants who entrusted them with their sensitive information. As Target, Home Depot, and many other companies can attest, data breaches are no joke, and the damages can be extremely far reaching in terms of economic and reputational harm.

Another concern for T-Mobile is their relationship with its partner entity and whether that relationship continues. The problem: The partner entity's principal line of businesses includes credit services. This means the company collects information on people, businesses, motor vehicles, and insurance; and many companies use the partner entity to determine if a customer has a good enough credit score to extend that person credit. As such, there are only a couple alternative companies T-Mobile can go to for this type of work. In addition, not only is the partner entity's relationship with T-Mobile on the line, but other companies that use the partner entity have reason to be concerned as well.

Takeaways

As we advise clients all the time, the first step in data privacy is making sure the company's own network is secure. The second necessary step is making sure those you work with, whether it be vendors, third-party contractors, etc., are doing the same. While vendor agreements can go a long way in terms of structuring the relationship between a company and a vendor, including calling for heightened security requirements, they cannot prevent a breach. They can, however, detail what happens in the event of a breach of the vendor's information systems that may lead to a breach of the company's information. In order words, take vendor contract management seriously and have an attorney who is familiar with data privacy issues review vendor and other third-party agreements to ensure the company is taking all precautions at its disposal to reduce the ramification of a data breach.