05/06/2014

By: Mark Pribish, special to the Arizona Republic, April 3, 2014, used by permission of the author

Americans are spending more on identity-theft services largely centered on alerts and monitoring, yet reported ID and data theft incidents are at near historic high levels. Target's data breach debacle has increased the debate on whether identity theft services can prevent consumers from becoming victims and if these services are worth the cost.

Extensive marketing by leading retail sellers of consumer identity theft services have led Americans to believe that monitoring and alerts mitigate or eliminate the chances of becoming an ID theft victim. Contrary to these ad claims are published reports showing increased consumer spending for prevention and the continuing meteoric rise in ID-data theft incidents.

No one suggests services that aim to protect consumers from identity theft are without value, but the benefits seem limited.

Javelin's Strategy & Research Identity Fraud Report from February reports that spending for ID thefts alert and monitoring isn't working "as advertised," with victim numbers up. There were 13.1 million identity theft victims in 2013 – the second-highest total ever. The third-highest total was recorded in 2012.

What's my point? More consumers are purchasing more identity theft alert and monitoring "protection" than ever and yet there are more victims of identity theft.

Besides credit and financial ID fraud plaguing Americans, identity theft includes account takeover, medical and taxpayer identity theft. It's time to look at ID and data theft consumer protection like car insurance. When there's a wreck, insurance pays to fix the damage and makes the vehicle like it was before the collision. Likewise, if consumers choose to purchase ID protection, they need services that fix their ID theft "wreck" after their IDs are "hit" by criminals.

What should you do? Assume you will be an ID Theft victim. Take more responsibility and do more in protecting your personally identifiable information. Be more careful in giving out information and vigilant on ID issues. Use stronger passwords, update security software and shred sensitive documents.

Of course, none of this will protect you when a business, agency or an employer who has your personal information has a breach and your private data gets stolen and used. The key is, in addition to ID theft alerts and monitoring, consider buying or requiring those whom you do business with to provide ID theft restoration — a protection where one's ID is "fixed" by professionals after an ID has been acquired and misused by a third party.

Mark Pribish is vice president and ID Theft Practice Leader at Merchants Information Solutions Inc., an ID Theft-Background Screening company based in Phoenix.