IDShield®

Responding to a Data Breach Event

You may have been following news of recent data breaches that have compromised sensitive customer information, potentially exposing victims and their families to identity theft. Last year millions of consumers had there personal information exposed due to data breach incidents.

Most of us have received a notification from our bank, health care provider or credit card company. This is a cause for concern, and the question then becomes, "Just how concerned should I be?" and "How should I respond?"

Breach notifications from banks, health care providers or credit card companies often bring with them an offer of a temporary identity theft product 12 to 24 months. But it's important to consider what these temporary services may not cover:

- Restoration services available through an offer from the breach entity usually only apply to a matter connected to the breach event itself.
- Today's data breach can lead to repeated identity theft incidents in the future, as thieves typically use such data more than once. This underscores the need for longterm monitoring.
- Temporary services may not include a personal investigator, nor the guarantee of comprehensive identity restoration.
- An online password protection using military-grade encryption. Temporary services may not include an online password manager.

When it comes to identity theft, the best approach is to have a product in place before the next incident happens.

To learn more about LegalShield's IDShield services, contact a LegalShield Independent Associate in your area or visit idshield.com.

Identity theft protection starts with having a service in place that allows members and their families to detect and respond to an event involving personal identifiers.