

# Frequently Asked Questions

IDT911 provides your business customers with the most comprehensive solutions in the industry to help offer appropriate response and assistance to those impacted by a data breach.

## ▶ WHAT IS A DATA BREACH?

A data breach is a security incident in which **sensitive, protected or confidential data is intentionally or unintentionally released to an untrusted environment.**

Lost data may involve personal information (PII), such as Social Security number, financial information such as credit card or bank details, and personal health information (PHI).

## ▶ WHY WOULD I WANT MY POLICYHOLDER TO CONTACT THE BREACH TEAM?

The **breach services team** is ready to

- Assist with **crisis management, answering questions, and listening to any concerns** the policyholder might have.
- Provide **necessary documentation**
- Assist in **drafting breach notices**
- Provide **industry best practices** regarding the handling of a breach.

## ▶ WHAT DO CLIENTS DO WHEN THEY THINK THEY'VE HAD A BREACH?

- **At the first sign of a breach**, or when your policyholders have a breach related question or concern, they should call your claims department at **866.351.3046.**
- Once their eligibility is verified, their basic contact information is taken and provided to an IDT911 breach consultant.
- The breach services team contacts the policyholder within one business day.

## ▶ WHAT IF AN EMPLOYEE OR POLICYHOLDER CALLS ME DIRECTLY FOR HELP?

Instruct the policyholder to call the claims department at **866.351.3046**

**A company laptop is missing, customers' payment records stolen, paper files are lost, online systems hacked...**

### THE FACTS\* ON DATA BREACHES

- 74% of small and mid-size businesses were targeted for cybercrime
- 42% lost confidential or private data
- 40% experienced direct financial costs due to attacks
- Average cost of the attack was \$188,242

\*Symantec 2010 Global SMB Information Survey

### ABOUT IDT911

Protecting more than 30 million Americans, IDT911 is a leader in identity management and identity theft remediation and resolution services to businesses and consumers on behalf of its 450 client institutions, as well as in comprehensive data breach preparedness (including incidence response plans), compliance, and notification and remediation services that are currently found in more than 150,000 businesses.

Powered by



# Frequently Asked Questions

## ▶ WHAT MAKES OUR DATA BREACH OFFERING UNIQUE?

We make this coverage available as an endorsement to our business owner's policy vs. a stand-alone policy.

Our offering **includes proactive and post-breach services** to help minimize the occurrence of a data breach and expert assistance if one occurs.

## ▶ HOW DOES THIS OFFERING HELP ME?

- Grow your businesses by attracting new customers and retaining existing ones
- Reinforce your role as trusted advisor with solutions to this emerging risk
- Minimize E&O exposures

## ▶ IS THE BREACH SERVICES CONSIDERED INSURANCE?

No. These services should be classified as a **“value added” feature** available as part of the larger policy offering.

And because these services are not considered insurance coverage, policyholder and employee usage of these services will not impact any policy loss ratios.

## ▶ WHAT IS THE BREACH WEBSITE?

**Co-branded Data Breach website** access

- Available at [www.capacityinsurance.breachresponse.com](http://www.capacityinsurance.breachresponse.com)
- Username: **Capacity1**
- Password: **Capacity1**
- After login you'll be required to create your own, unique username and password

## ▶ CONSIDER THE FOLLOWING WHEN UNDERWRITING COVERAGE...

- Does the company collect and store sensitive information?
- What type of sensitive information do they store?
- How many records do they collect with PII involved?

## SERVICE OVERVIEW

The IDT911 breach experts will:

- Help determine the extent of the situation and next steps
- Work closely with the policyholder and the claims department to facilitate the process
- Assist policyholders in developing the required breach victim notifications and industry best practices to respond to a breach
- Work with your policyholders to organize their media response
- Provide expert case handling from first call to remediation with built-in identity theft resolution for all affected individuals

What background does the breach Services team have?

The breach services team has multidisciplinary backgrounds in:

**Data Security**  
**Computer Forensics**  
**Privacy Law**  
**Information Technology**  
**Business Administration**

Powered by

