# Help your customers understand the importance of data breach coverage.

## Spectrum®

Many small businesses are vulnerable to data breaches. Yet, their owners don't think they need specific data breach protection. Use this guide for:

- **Data breach coverages we offer –** including limits and deductibles
- **Resources from The Hartford Cyber Center –** to help customers prepare for and deal with a breach
- **Real-life claim scenarios –** an effective way to persuade customers that a data breach could occur at their business

### Easy Add-on Endorsement

When quoting, remember that it's easy to add data breach coverage as an endorsement to our Spectrum Business Owner's Policy.

## Data Breach Coverage Overview

### First-party Response Expense Coverage

- Legal and forensic services for breach investigation
- Crisis management
- Notification of impacted parties (including writing and mailing)
- Public relations and good faith advertising (to help protect and/or restore a business's reputation)
- Credit monitoring for impacted parties (if warranted)
- Limit options: $10K | $25K | $50K | $100K | $250K | $500K | $1M
- Deductible options: $1K-$100K available; minimum deductible rules apply

Optional Coverages

- Extortion Threats
- Business Income and Extra Expense

### Third-party Defense and Liability Coverage

- Provides coverage for civil awards, judgments or settlements a business is legally obligated to pay arising from a data breach claim
- Provides defense coverage for regulatory proceedings
- Limit options: $50K | $100K | $250K |$500K | $1M[1]
- Deductible options: $1K-$100K available; minimum deductible rules apply

Optional Coverages

- Fines and Penalties
- PCI (Payment Card Industry) Loss

Note: For state exceptions, refer to the Spectrum Product Manual.

The Hartford

## The Hartford Cyber Center

Through this center, we offer tips, guidance and resources to help business customers:

- Minimize the chance for a breach
- Safeguard Personally Identifiable Information (PII)
- Become aware of legal requirements by state
- Create a data breach incident response plan
- Understand what to do if a breach occurs
- Access a team of experts that can:
  - » Assist if a customer believes a breach has occurred
  - » Determine breach severity
  - » Consult on "next steps" to address a breach situation

## Data Breach Claim Scenarios

Here are some claim scenarios that show how we respond to a data breach claim. Use these scenarios in conversations with your small business customers to illustrate:

- The real risk of a data breach
- Their need for data breach coverage

| Scenario 1 | |
|---|---|
| **Type of claim** | Data breach |
| **Policy type** | First-party Response Expense and Third-party Defense & Liability Expense |
| **Cause of action** | Stolen laptop; failure to encrypt Personally Identifiable Information (PII) |
| **Type of insured** | Financial services company |
| **Facts** | **Situation:** Lilly Backus, an employee of a financial services company, attends a conference on behalf of her employer.<br>During the conference, her laptop is stolen. Knowing that the personal information for her clients, including Social Security numbers, is stored on the laptop, she immediately contacts her employer to report the theft. Lilly is hoping that, because the laptop was password protected, her clients' personal information is not at risk.<br>Unfortunately, Lilly never 'encrypted' the data.<br>**The insured's actions:** After receiving a report of the alleged theft, Lilly's employer immediately contacts us to report that a data breach occurred. Fortunately, they had recently purchased First-party Response Expense and Third-party Defense & Liability coverage.<br>**Our actions:** After gathering facts about the incident, one of our claims representatives contacts a panel law firm to review the report and determine appropriate next steps.<br>Counsel recommends using forensic services to investigate the loss and determine whether the password protection function of the specific model of Lilly's computer provided adequate safety for the client records or encrypted the laptop contents. (The forensics firm was on our panel of vendors.) |
| **Conclusion** | It was determined that:<br>• A data breach occurred • The data was stolen • Coverage was available |
| **Services triggered** | • Investigated the loss; this included using forensic services<br>• Provided counseling on state notice requirements<br>• Mailed notification letters to breach victims<br>• Provided credit monitoring services for the breach victims up to one year, helping to mitigate the potential for a third-party claim |
| **Coverage response** | First-party Response Expense triggered<br>$15,000 for Notification Expenses and Credit Monitoring Services<br>$5,000 for Forensic Expenses<br>$20,000 Total Loss Paid |

| Scenario 2 | |
|---|---|
| **Type of claim** | Data breach |
| **Policy type** | First-party Response Expense |
| **Cause of action** | Computer hacking |
| **Type of insured** | Electronics equipment retailer |
| **Facts** | **Situation:** Jones Electric is a retailer of electronic equipment, including TV, radio and computers. Jones thinks that their computer system was hacked, causing it to divulge credit card numbers for several of their customers, as well as Social Security numbers from credit applications.<br>**The insured's actions:** Mr. Jones contacts us to report that a data breach occurred.<br>**Our actions:** One of our claims representatives:<br>• Verifies that Mr. Jones had purchased First-party Response Expense coverage<br>• Contacts a panel law firm to review the claim and determine appropriate next steps<br>Counsel recommends using forensic services to investigate the loss. |
| **Conclusion** | Upon review, it was determined that:<br>• A breach occurred due to an employee error<br>• An employee had failed to log off from his computer when going to the back room<br>• An unknown individual accessed and downloaded customer credit card and customer credit application information<br>Counsel and panel vendors also provided services that involved:<br>• Assistance with preparing and mailing notification letters to impacted individuals<br>• Determining if any monitoring services should be offered<br>**Outcome:**<br>• We covered these expenses through our Spectrum® First-party Response Expense coverage<br>• The insured was able to mitigate the potential of a third-party claim because of the appropriate actions taken to notify individuals of the breach, and support services provided, like credit and fraud monitoring services |
| **Services triggered** | • Investigated the loss; this included using forensic services<br>• Provided counseling services on state notice requirements due to the data breach<br>• Mailed notification letters to breach victims<br>• Provided credit monitoring services for the breach victims up to one year, helping to mitigate the potential of a third-party claim |
| **Coverage response** | $5,000 for Notification Expenses and Credit Monitoring Services<br>$5,000 for Forensic Expenses<br>$10,000 Total Loss Paid |
| **Scenario 3** | |
| **Type of claim** | Data breach: third-party claims |
| **Policy type** | First-party Response Expense and Third-party Defense & Liability Expense |
| **Cause of action** | Computer hacking |
| **Type of insured** | Business consultant |

continued

| Scenario 3 | |
|---|---|
| **Facts** | **Situation:** An unknown person hacks into the personnel files for employees of Harken Enterprises.<br>The files included the full name and addresses of their employees, as well as Social Security numbers.<br>**The insured's actions:** When Hank Lindell, an employee of Harken, reports suspicious new accounts on his credit files, Harken contacts us to report the incident.<br>**Our actions:** One of our claims representatives:<br>• Verifies that Harken had purchased First-party Response Expense and Third-party Defense & Liability coverage<br>• Contacts a panel law firm to review the claim and determine appropriate next steps<br>Our actions: One of our claims representatives:<br>• Verifies that Harken had purchased First-party Response Expense and Third-party Defense & Liability coverage<br>• Contacts a panel law firm to review the claim and determine appropriate next steps |
| **Conclusion** | After reviewing the specifics of the reported incident and conducting an investigation, counsel and panel vendors provided services that involved:<br>• Assistance with preparing and mailing notification letters to impacted individuals<br>• Determining that credit and fraud monitoring services should be offered<br>• Providing assistance to Harken in preparing a media response to regain employee and con-sumer trust after word of the data breach had spread<br>**Outcome:** Despite the credit and fraud monitoring services made available to them, several employees filed suit against Harken Enterprises for damages they claimed to have incurred as a result of the breach.<br>Their suit included claims for emotional distress resulting from the data breach.<br>Our claims handler confirmed that Harken had purchased a First-Party Response Expense and Third-Party Defense & Liability policy, and that the claims asserted in the suit were cov-ered under the policy.<br>We then retained a panel counsel to defend Harken Enterprises. The defense attorney ob-tained a favorable outcome and we were able to settle the matter for a modest payment. |
| **Services triggered** | • Investigated the loss<br>• Provided counseling services on state notice requirements due to the data breach<br>• Mailed notification letters to breach victims<br>• Provided credit and fraud monitoring services<br>• Paid for defense counsel and settlement amount |
| **Coverage response** | $5,000 for Forensic Expenses<br>$10,000 for Notification Expenses and Credit/Fraud Monitoring Services<br>$5,000 for Good Faith Advertising<br>$100,000 for Third-Party Defense & Liability<br>$120,000 Total Loss Paid |

**Talk to your customers** about adding data breach coverage.

The Hartford

[1] Available options may vary by type of business and state