TRIDENT
PUBLIC RISK SOLUTIONS

Member Argo Group

Data Compromise 360© Helps Local Governments Respond to Data Breaches

TRIDENT PUBLIC RISK SOLUTIONS REMAINS COMMITTED TO PROVIDING SECURITY COVERAGE FOR TODAY'S PUBLIC ENTITIES.

Data Compromise 360© is an insurance solution provided by Trident that is designed to help local governments respond to data breach incidents involving employee or client information that was stolen, electronically hacked, or lost through an accidental or inadvertent release.

Data Breaches: A Growing Public Issue

Concerns about data breaches are so great that most states now have laws requiring governments to notify those affected. But beyond what's required, public entities need to ensure they're protecting their own reputation after a breach occurs.

Meeting This Growing Need

Data Compromise 360© was designed to help local governments respond to the financial burden and service obligations a data breach can cause.

Public entities must be able to notify all affected parties and effectively communicate the scope of the possible damage. They may also be required to provide credit monitoring assistance and other restorative measures to those affected by the breach.

Coverage Highlights, Terms and Conditions

The discovery of a personal data breach triggers this coverage, which includes:

- Payment of first-party expenses incurred from responding to a personal data breach. That includes outside legal counsel, a forensic IT review, public relations costs, notifications, reimbursement for fines and penalties, and credit monitoring and other services for those affected.
- Defense and liability costs for actions brought by those impacted or government entities.

Data Compromise 360© covers the following types of events.

- Loss or theft of electronic or physical files, accidental release or publication, as well as voluntary release due to fraud.
- Lost data must have been in the care, custody or control of the insured or a third party with whom the insured has a direct relationship and has directly turned over such data.

Public entities can also take advantage of these other Data Compromise 360© services.

- With this coverage comes access to eRiskHub®, a risk management portal designed to help local governments prepare and respond effectively to data breaches. Key features of the eRiskHub® portal include an incident response road map, online training modules, risk management tools to manage data breaches, a directory for external resources, a news center with current articles from industry resources, and a learning center with best practices and white papers.
- Services also include access to experts in data compromise and breaches.
- Claims are managed by experienced and dedicated data compromise specialists with industry knowledge.

TRI-7812-032018

TRIDENT
PUBLIC RISK SOLUTIONS

Member Argo Group

Data Compromise 360© Coverage Overview

Availability

Data Compromise 360© is available as additional policy coverage that's part of Trident's public entity package. Coverage is provided on a claims-made basis.

Eligibility

Most public entities are eligible for Data Compromise 360©.

Exclusions

Date of breach may not be prior to first inception of the coverage. No coverage is provided for insured's criminal acts or reckless disregard for data security.

Coverage Terms

- Data compromise 360© response expense
  - Options: $100,000, $250,000, $500,000 and $1 million
  - Sublimits:
    - Forensic IT: 50 percent of the data compromise response expenses limit
    - Legal review: 50 percent of the data compromise response expenses limit
    - Public relations: $5,000
    - Regulatory fines and penalties: 50 percent of the data compromise response expenses limit
    - PCI fines and penalties: 50 percent of the data compromise response expenses limit
    - Named malicious code: $50,000
- Data compromise 360© liability
  - Options: $100,000, $250,000, $500,000 and $1 million
  - Named malicious code: $50,000 per occurrence
- Deductibles
  - Data compromise 360© response expense:
    - $1,000 for $100,000 limit
    - $2,500 for $250,000 limit
    - $10,000 for $500,000 limit
    - $10,000 for $1 million limit
  - Data compromise 360© liability:
    - $1,000 for $100,000 limit
    - $2,500 for $250,000 limit
    - $10,000 for $500,000 limit

Claims Examples

Who: school district

What: A spear phishing email purportedly from a district superintendent resulted in the release of personally identifiable information on more than 1,500 employees.

Cost: $125,000 for breach notification and identity protection

Who: parks and recreation

What: A laptop containing personally identifiable information on 250 summer sports registrants was stolen from an office.

Cost: $25,000 for credit reporting and monitoring

Who: local utility service

What: A city's online utility payment system was breached, potentially exposing credit card data from more than 40,000 customers.

Cost: In excess of $100,000

TRI-7812-032018

Solutions for Your Challenges

Public entity clients count on you to keep them protected from today's risks and challenges. You can depend on Trident to keep them up to date with contemporary coverage and services that keep you a step ahead of the competition.

Contact your Trident representative today for more information about Data Compromise 360©.

Visit www.argolimited.com/trident/contact to see a staff directory.