DATA PRIVACY & SECURITY

DataBreach℠ for Insurance Professionals

Classes We Consider

- Claim adjusters
- Insurance carriers
- Insurance brokers
- MGAs
- Premium audit vendors
- Retail agents
- Third party administrators

Assess the Risk Reality

- Does the company use portable "jump" or "thumb" drives to transport files and information?
- Is every business laptop encrypted?
- Are backup tapes used and carried off-site?
- Does the emerging threat of healthcare benefits fraud pose a risk to the business?
- Does the business owner realize that, although employees' access to sensitive data may be monitored, the way they use that data is impossible to control?
- Has anyone in the business ever been asked to give out their password over the phone to diagnose a technical problem they have been having?
- Does the business use the services of third parties for data storage, IT systems support or management, collections or claim processing?
- Are paper records containing sensitive information stored securely and shredded before disposal?

What Does DataBreach℠ Offer?*

- Regulatory defense with no sub-limit and includes the portion of privacy regulatory settlements or judgments used to fund the payment of patient or consumer claims
- Coverage includes liabilities arising from the theft or loss of paper records
- Vicarious liability for data entrusted to Business Associates or other third parties (by endorsement)
- Liability from identity theft
- Media coverage for information on the business website, including whitepapers and content
- Recovery costs and extra expenses due to unauthorized access to data systems
- Punitive damages (when insurable by law)
- Claims made form
- Coverage through an insurance partner with a stable history in Agents & Brokers E&O
- Limits up to $10 million
- Supplementary payments coverage in addition to the limits, and not subject to the deductible, is included for compliance with security breach notice laws, voluntary credit monitoring, and public relations expenses
- **Forensic/incident response services from Fishnet Security as part of our claim handling process**

DATA PRIVACY & SECURITY

DataBreach℠ for Insurance Professionals

Receive cash for breach mitigation expenses, public relations, client notification, and voluntary credit monitoring with DataBreach℠ coverage.*

DataBreach℠ coverage, while it will not pay for fines, does offer coverage for defense of regulatory actions which is not subject to a sub-limit.*

Insurance related businesses are repositories of a rich store of confidential consumer information, which makes them top targets for data thieves. Carriers, brokers and agents are all vulnerable to a data breach, which can result in expensive lawsuits, loss of reputation and revenue.

With data breach on the rise, insurance professionals need to protect themselves against theft of policyholders' confidential information. While Markel's new DataBreach℠ information risk insurance coverage can't stop a breach from occurring, it can help an insurance related business pick up the pieces after one has occurred.

In the News

- Personal information on 72 Workers's Compensation claimants was stolen from Sentry Insurance and later sold over the Internet. Data on an additional 112,198 claimants was also stolen, but there was no evidence it was sold. The data sold included names and Social Security numbers but not medical records.[1]
- A data theft that was averted is no less troubling. Hundreds of documents containing confidential information were discovered in a dumpster belonging to Texas Insurance Claims Service. The files that were discovered contained names, Social Security numbers and insurance policy numbers, and was described by one witness as, "a gold mine for identity thieves." When contacted, the company said it uses commercial shredding services to dispose of policyholders' records but did not do so this time.[2]
- A New York banking insurance services company was recently affected by a home burglary in Florida. A consultant the company hired lost his laptop computer to thieves who broke into his home. The laptop contained personal information of the company's clients, including names, Social Security numbers, and some personal health information.[3]
- A computer server was recently stolen from a major insurance company, putting at risk nearly one million people who had personal data stored on the server. The data on the server included Social Security numbers and medical records of prospective customers, and had been forwarded to the server from insurance brokers around the country.
- A laptop computer containing personnel information was stolen from the Harrisonburg City, Ohio school system. The data stored on the laptop came from employees who enrolled in the system's dental plan. The laptop belonged to an outside insurance sales representative who was using the data to develop an insurance proposal for the school system.[4]

1, 2, Compiled from data at www.datalossDB.org

3 New York Regulator Notice, April, 2007

4 Compiled from www.privacyrights.org/ar/chrondatabreaches

*Coverage available through Markel regional offices: Markel Midwest, Markel Mid South, Markel Northeast, Markel Southeast and Markel West. For information refer to www.markelcorp.com. For complete terms and conditions, refer to the policy itself. Coverage is subject to conditions and exclusions in the policy.

BOLTON & COMPANY

Tracking down the right coverage for over 45 years.

2400 Waterfront Plaza · 325 West Main Street · Louisville, Kentucky 40202
Telephone 502.583.8361 · 800.292.6597 · Fax 502.584.6131 · www.boltonmga.com