

FINANCIAL INDUSTRY/INSTITUTIONS INCLUDING INSURANCE



PROFILE OF CLIMATE

Gramm Leach, Sarbanes Oxley and Secure Data laws have passed in 45 states. Additional legislations such as Red Flag rules, Patriot Act, FACTA, PCI Rules and others, have forced a very difficult standard of care upon the financial industry to protect consumer's proprietary information.

Legislative mandated breach reporting and compliance is now an extremely costly business expense - an average claim for secure data breaches is approx \$6.6 per incident and \$202 per client record. Breaches can result in class action suits at a magnitude never before seen in the financial industry (*Ponemon Institute Study*).

COVERAGE OVERVIEW

Claims made policies with Premiums ranging from \$5k to over \$1million for more complex coverage typically requiring worldwide coverage. Limits range from \$250k to \$25million and deductibles from \$1k upward to \$100k.

COVERAGE AVAILABLE

Cyber coverage for 1st and 3rd party malicious code

Secure Data coverage for breaches of GLB 401c, HIPAA, and states secure data laws

Business Interruption for loss of revenue during security breach crisis

Crisis Management reimbursement to remediate and control the incident including PR spin and media costs

Intellectual Property for perils like trademark, copy write and patent infringement

Errors and Omissions for malfeasance of the technology implementation team and their subcontractors associated with any professional technology service for a fee

Personal Injury to cover defamation, invasion of privacy or related perils

Call Center Support for costs associated with Q&A load from breached clients

Legislative Compliancy for certain fines and costs associated with investigations and penalties

CLASSES OF FINANCIAL COMPANIES

Class include, but are not limited to, mortgage brokers and banks, commercial banks, credit lenders of any type, funds, credit card transactions, financial planners, REIT's, Insurance companies, Insurance agents, MGU, TPA, MGA and all credit card companies.

QUESTIONS ABOUT YOUR INSURED'S

- Any secure data breaches or incidents in last 5 years?
- Do they have any compliance certificates (PCI, HIPAA, etc)?
- Do they collect and keep any proprietary info (SS#, Credit card info, Financial info, account numbers, maiden names, pets names etc)?
- Do they encrypt data, on laptops, back ups, emails etc. What is the sophistication of encryption?

- Do they use any wireless networks any where ?
- Do they have a security leader or CSO (Chief Security Officer)?
- Do they have any policy or procedures for identity theft or secure data breaches?
- Do they have any patents, copywrite, trademarks or intellectual property?
- Do they have a transactional website in any way?
- How often do they change passwords for their systems and do they contain a combination of letters and numbers?
- Do they have a POS, MAC machines?
- Do they do business in multiple states and or worldwide?
- Have they incorporated FACTA Red flag rules?
- Do they have a minimum of 2 locked doors with FOB or pass card protection at minimum and explain more complex security measures?

CLAIMS EXAMPLES

Choicepoint: The agency charged that ChoicePoint violated the FTC Act by making false and misleading statements about its privacy policies [Choicepoint had publicized privacy principles that address the confidentiality and security of personal information it collects and maintains] .

At Least 800 Cases of Identity Theft Arose From Company's Data Breach [financial records of more than 163,000 consumers in its database had been compromised]

The settlement requires ChoicePoint to implement new procedures - must establish and maintain a comprehensive information security program and to obtain audits by an independent third-party security professional every other year until 2026.

Insurance Agent: CS Stars, an independent insurance brokerage; says the names, addresses, and SSN's for 540,000 injured workers may have been lost.

Insurance Company: Wellpoint [health benefits company] said two computer servers on which the records were stored were maintained by a third party vendor and were not properly secured between 2007 and 2008. 130,000 customers' protected health information, personal records, and SSN's have been exposed over the internet for an unspecified period of time.

Processing Company: Between 2004 to present, CardSystems is facing a class action lawsuit over security breach which may have exposed 40 million credit card numbers to fraud.

Source:

<http://www.privacyrights.org/ar/ChronDataBreaches.htm>