

# Enterprise Privacy Protection Insurance

## Designed for Financial Institutions

**Liability insurance to cover you following a breach of privacy or computer network security, including crisis management and customer notification expense**

Privacy and security related risks are a boardroom issue and expose financial services organisations to regulatory enforcement actions, liability claims and, in some cases, direct losses. Traditional insurance policies are inadequate in this modern environment and these new forms of risk could have severe financial consequences.

Enterprise Privacy Protection has been designed to help fill these insurance cover gaps. The policy is underwritten by Lloyd's of London and was first introduced in March 2005.

## Main Insuring Clauses Enterprise Privacy Protection

Section	Sum Insured
<p><b>A. Third Party Privacy Liability</b> Sums the insured is legally obligated to pay as damages and claims expenses as a result of a privacy breach or breach of privacy regulations. The definition includes common law breach of confidence, HIPAA, Gramm-Leach-Bliley Act, privacy protection laws and privacy provisions of the Federal Fair Credit Reporting Act.</p>	US\$ Policy limit Any one claim and in all during the policy period.
<p><b>B. Employee Privacy Liability</b> Same as coverage A but the plaintiff is an employee (excluding claims arising out of employment practices liability or ERISA violations).</p>	US\$ Policy limit Any one claim and in all during the policy period.
<p><b>C. Privacy Regulatory Defence and Penalties</b> Defense of a regulatory action, complaint, investigation including indemnification for a penalty, civil fines, or sanction imposed by a federal, state or regulatory body, as a direct result of a privacy breach or breach of privacy regulations as defined.</p>	Up to US\$1,000,000 Any one claim and in the annual aggregate limit of insurance. Subject to pre-agreed coinsurance participation.
<p><b>D. Crisis Management and Customer Notification Expenses</b> Cover for:</p> <ul style="list-style-type: none"> <li>• public relations services to protect brand/image related to a claim, penalty, civil fines or sanction covered under the other insuring clauses</li> <li>• notification expenses to warn customers or patients of security breaches as required by many state laws.</li> </ul>	US\$2,000,000 Any one occurrence without application of any policy
<p><b>E. Security Liability</b> Sums the insured is legally obligated to pay as damages and claims expenses arising out of computer attacks caused by failures of security including theft of client information, identity theft, negligent transmission of computer viruses and denial of service liability. Broad coverage is provided to address insiders as perpetrators and provide coverage for "failure to warn" obligations created by state laws, such as the California Data Protection Act (SB1386).</p> <ul style="list-style-type: none"> <li>• Affirmative coverage for "phishing" and "pharming" i.e. false communications designed to obtain personal information.</li> <li>• Security coverage extends to the protection and confidentiality of all customer records or information, not just that contained in computer systems.</li> <li>• Contractual coverage for breach of the insured's privacy statement.</li> <li>• Expanded definition of "privacy breach" and "privacy regulations". Basically follows what a regulator deems to be privacy rather than a more limited insurer definition.</li> </ul>	US\$ Policy limit Any one occurrence and in all during the policy period.

## Key cover features of Privacy and security risk background

### Why this is a boardroom issue

Financial services organizations perform innumerable transactions and infrastructure functions through public and private networks, including new wireless applications. Increasing dependence on technology, outsourced providers and internet based services mean that the computer networks of financial services companies are under constant threat. Major IT security issues include unauthorized access or use of computer networks, identity theft, spyware, denial of service attacks, phishing, and malicious code. Perpetrators of security breaches may well be inside employees or independent contractors in the US or overseas. Reputation and business risks are extensive,

particularly for entities subject to the accountability and internal control requirements of the Sarbanes-Oxley Act. There are a of variety of regulations that have been established to increase protection of financial and personal data. Gramm-Leach-Bliley Act of 1999 (G-L-B) imposes major privacy and security requirements on financial services companies engaged in financial transactions and communications. The law limits the instances in which financial institutions may disclose non-public personal information about a consumer to non-affiliated third parties and requires them to disclose certain privacy policies and practices to all of its customers. G-L-B, also, requires

financial institutions to have a security plan to protect the confidential integrity of customer information. Some financial services companies may also be subject to privacy requirements for personal health information (regulated by HIPAA). Certain states have passed consumer data protection laws, such as the landmark California Database Protection Act of 2003 (previously called SB 1386) requiring notice to affected customers upon discovering a breach of defined personal data – over 40 states and the District of Columbia have now passed similar laws.

## Technology Liability and Cyber Risk Experts

JLT has a specialist Technology Liability and Cyber Risks team advising many leading corporations around the world and providing specialist access to the London insurance market.

## Other Technology and Cyber Risk Products

JLT has developed a range of Technology and Cyber Risk products providing third party liability, first loss property and business interruption coverage.





## Why purchase Enterprise Privacy Protection?

Traditional insurance policies do not usually provide adequate protection. Crime policies generally do not cover stealing data or consequential damages. The Commercial General Liability (CGL) policy has limited coverage for privacy claims related to an Insured's own publishing and advertising activities. Courts have held that data is not "tangible property"; therefore liability arising out of theft of third parties' electronic data would typically not be covered by a CGL or Property policy. "Intentional acts" exclusion within Professional Liability policies eliminates coverage if insiders/employees are hackers. Generic cyber

liability products may not address the scope of coverage needed for privacy and security risks following the regulatory requirements and typically exclude coverage for regulatory, fines and penalties complaints.

### To find out more contact:

#### **Simon Milner**

+44 (0) 20 7558 3647  
simon\_milner@jltgroup.com

#### **Warren Hattwich**

+44 (0) 20 7558 3457  
warren\_hattwich@jltgroup.com

Or visit our web site

<http://www.jltgroup.com/it-risk-assessment>

This document is for information only and in no way overrides or forms part of any Enterprise Privacy Protection policy. It does not constitute an offer of insurance of any kind, nor should it be relied upon as a description of precise coverage which may be available under any Enterprise Privacy Protection policy. If you would like to see a full copy of the standard policy wording please contact [simon\\_milner@jltgroup.com](mailto:simon_milner@jltgroup.com).

### **JLT Specialty Limited**

6 Crutched Friars  
London EC3N 2PH  
Tel +44 (0)20 7528 4000  
Fax +44 (0)20 7528 4500  
[www.jltgroup.com](http://www.jltgroup.com)

Lloyd's Broker. Authorised and Regulated by the Financial Services Authority. A member of the Jardine Lloyd Thompson Group. Registered Office: 6 Crutched Friars, London EC3N 2PH. Registered in England No. 01536540. VAT No. 244 2321 96.

© January 2011 262915