CYBER INSURANCE

The Cyber Liability Insurance policy provides coverage for a wide range of cyber and privacy exposures through three core insuring agreements, four optional insuring agreements and two optional endorsements. Each insuring agreement and endorsement is designed to protect the key cyber risks faced by banks.

DATA BREACH LIABILITY

Data Breach Liability is the mainstay of privacy and cyber insurance, providing coverage for:

- The failure to prevent unauthorized access to both electronic and non-electronic confidential information (a data breach). The information may be in the care and custody of the bank or certain bank service providers.
- The failure to properly notify impacted parties of a data breach as required by law.
- Demands for restitution for lost business opportunities as a result of exposed confidential data by a victim of a breach incident.

FOR EXAMPLE

- The bank's payment system is hacked resulting in the unauthorized exposure of tens of thousands of confidential customer records. The records were subsequently misused as part of an identity theft scheme. The customers sue the bank demanding restitution for lost funds and expenses incurred in clearing their identities.
- The bank is sued for lack of adequate security measures after confidential customer information was stolen from a dumpster of discarded account files.
- A bank employee erroneously emailed portions of a customer database to an outside vendor. The vendor used confidential information found in the database to solicit business for its Florida timeshares. The bank's customers sue the bank for wrongful disclosure of private data.

NETWORK SECURITY LIABILITY

Network Security Liability provides coverage for the bank's E&O exposure arising out of network security intrusions such as distributed denial of service (DDoS) attacks and virus transmissions.

FOR EXAMPLE

- Demands are made against the bank for loss of business opportunity due to the loss of customer account access while the bank's online banking systems were disabled by a denial-of-service attack.
- Demands are made against the bank for system damage incurred after a customer received a virus from the bank's online banking platform.

CYBER PUBLISHING AND SOCIAL NETWORKING LIABILITY

Cyber Publishing and Social Networking Liability addresses gaps in defamation and similar coverage under a bank's General Liability policy by providing coverage for defamation and similar allegations arising from communications displayed or distributed through the bank's websites and social networking accounts, whether posted by the bank or someone else.

Coverage also addresses accusations of copyright infringement, misappropriation of ideas, slander and advertising injury arising from the bank's website and social networking accounts.

FOR EXAMPLE

- The bank unknowingly uses copyrighted art on its website. The American Society of Artists sues the bank for copyright infringement.
- A local resident sues the bank alleging it published her picture on the bank's Facebook page without her permission.

CYBER LIABILITY OPTIONAL INSURING AGREEMENTS

ELECTRONIC FUNDS TRANSFER LIABILITY

Electronic Funds Transfer Liability provides coverage when a demand is made against the bank in connection to the wrongful electronic transfer of customer funds. Coverage includes electronic funds transfer initiated by faxes, emails, phone calls or online banking.

FOR EXAMPLE

- Funds from a customer account are wired to a third party based upon a fraudulent instruction initiated using the stolen log-in credentials of a bank employee. The customer demands restitution.
- Funds from several customer accounts are wired overseas when hackers gain control of the bank's systems. The customers sue the bank to recover the lost funds.

REGULATORY DEFENSE

Regulatory Defense provides coverage for defense expenses incurred if regulatory proceedings are brought against the bank in connection with a data breach incident or wrongful cyber publishing act.

CLAIMS EXAMPLE

- After a data breach resulting in the exposure of confidential customer information, the bank's regulators allege that the bank had inadequate security controls. The regulators formally charge the bank with regulatory violations.
- The Office of the Comptroller of Currency took action against the bank for deceptively advertising free checking accounts. The agency found that the bank lured in customers with promises of "no strings attached" free checking, without disclosing key requirements.

BREACH RESPONSE EXPENSES

Breach Response Expenses indemnifies the bank for professional expenses incurred to investigate and possible data breaches or similar attacks. Professional expenses include:

- forensic investigations
- technological assistance required to restore access
- notification costs
- card reissuance
- credit and identity theft monitoring
- call centers
- legal counsel
- PCI and regulatory fines

CLAIMS EXAMPLE

A bank discovers that its online banking system has been breached over the course of three months. Thousands of customers had their confidential information stolen. The bank, on the advice of its data breach coach, hires a forensic investigator to determine the cause and extent of the breach, notifies the FBI and local authorities, notifies its customers, and provides all victims with credit and identity monitoring services.

PUBLIC RELATIONS EXPENSE

Public Relations Expense indemnifies the bank for expenses incurred to hire a public relations expert to help mitigate the reputational damage to the bank in the wake of an electronic or non-electronic data breach or any other claim covered under the policy.

CLAIMS EXAMPLE

A bank's mortgage loan office has their laptop stolen. The laptop contains hundreds of borrower records, including nonpublic, personally identifiable information. The bank hires a public relations firm to restore borrower confidence in the bank's ability to manage its security controls and customer data.

CYBER LIABILITY OPTIONAL ENDORSEMENTS

CYBER EXTORTION

Cyber Extortion indemnifies the bank for loss of property surrendered as a result of cyber threats.

FOR EXAMPLE

A bank decides to not extend credit to a business customer. In retaliation, the customer announces it has access to the bank's systems and threatens to shut down operations unless the bank transfers a large sum to its Cayman Island accounts. The bank receives reimbursement for monies surrendered to avoid the shutdown.

NETWORK INTERRUPTION

Network Interruption indemnifies the bank for lost income and additional expenses incurred when a bank's system stops functioning due to system breach or in response to a cyber extortion threat. Dependent System Failure is also covered at a sublimit.

FOR EXAMPLE

A hacker shuts down the bank's online banking platform. The website is down for 48 hours as programmers rewrite, test and elevate new code. In the interim, the bank extends hours at its branches to accommodate those who normally bank online in the evenings. The bank receives reimbursement for lost income and additional expenses incurred after the initial 24-hour downtime period.