CYBER LIABILITY INSURANCE

The Cyber Liability Insurance policy provides coverage for a wide range of cyber security and privacy exposures through seven integrated insuring agreements and two optional endorsements. Each coverage part 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 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.
- Confidential customer information was stolen from a dumpster containing discarded account files. The bank was subsequently sued for failure to safeguard private information.
- The bank stored its backup data with a third-party cloud service provider. The service provider suffered a system breach, resulting in the exposure of bank customer account information; however, the service provider did not notify the bank or its customers of the data breach until 7 months after the incident occurred. The bank was served with a class action lawsuit for failure to timely notify the impacted individuals.

POLICY DIFFERENCES

- Some policies exclude coverage for losses arising from the theft or unauthorized disclosure of non-electronic (paper) records.
- Some policies contain an encryption requirement, precluding coverage for claims arising out of breaches of unencrypted data.
- Some carriers exclude coverage for claims arising out of breaches at service providers or offsite computer systems. Be aware, in most cases, it is the data owner (the bank) that faces liability exposure from a data breach, even if the security failure is the fault of the data holder (service provider).

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.

POLICY DIFFERENCES

- Some policies require that the bank maintain adequate security measures. Failure to do so can nullify coverage.
- Some policies exclude coverage for loss caused by the malicious actions of employees.

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 for copyright infringement.
- A local resident sues the bank, alleging it published her picture on the bank's Facebook page without her permission.

POLICY DIFFERENCES

Some policies contain an exclusion for claims arising out of data collection practices or the distribution of spam.

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.

POLICY DIFFERENCES

Some policies do not provide liability coverage for the bank's errors and omissions related to electronic funds transfers.

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.

POLICY DIFFERENCES

Some policies contain a narrow definition of regulatory agency, excluding entities such as state attorneys general. This is problematic as most privacy laws are governed by these state offices.

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 discovered that its core banking system was breached over the course of three months. The bank, on the advice of its data breach coach, hired a forensic investigator to determine the cause and extent of the breach. The investigator found that 11,000 customer plastic card records were exposed. The bank notified all impacted customers, provided them with credit and identity monitoring services, and reissued all 11,000 plastic cards with new account numbers.
- The bank's online banking service provider experienced a major data breach, exposing the confidential information of thousands of bank customers. As the owner of the data, the bank had a legal obligation to provide an adequate and timely notice of the data breach to its impacted customers. The bank issued 7,500 notification letters to customers in 4 states.

POLICY DIFFERENCES

- Some policies do not cover the expenses incurred to change account numbers and reissue plastic cards for persons impacted by a data breach.
- Some policies will not cover the costs of notification for data exposed through a third-party service provider, even if the bank owns the data.

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.

POLICY DIFFERENCES

In addition to public relations expense reimbursement, some carriers may offer optional reputational loss coverage—reimbursement for incremental profits that were lost due to reputational damage from certain cyber events.

CYBER LIABILITY OPTIONAL ENDORSEMENTS

CYBER EXTORTION

Cyber Extortion indemnifies the bank for loss of property surrendered in response to a cyber threat.

FOR EXAMPLE

A threat actor electronically announces to the bank that it has encrypted the bank's systems and threatened to expose customer data unless the bank transfers a large sum to a Cayman Island bank account. The bank receives reimbursement for the money surrendered to restore its systems and avoid the dissemination of private customer data.

POLICY DIFFERENCES

- Some policies only cover extortion events involving system shutdowns but not threats of data exposure. Increasingly, threat actors are stealing data with threat of publication.
- Some policies require that the extortion threat be made by a "natural person," potentially precluding coverage for actions by any formal organization or entity. It may also preclude coverage when the attacker is unknown.

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, system failure, 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 scheduled downtime period.

POLICY DIFFERENCES

- Some policies only cover outages resulting from malicious hacks into the insured's system, precluding coverage for an outage related to system failure.
- Some policies won't cover an intentional outage brought about by the bank in an attempt to protect its computer systems or secure confidential information from an active or imminent extortion threat.