

Fidelity Loss Scenarios



Insurance Company - Adjuster Fraud

Description of Event:

Our insured, an insurance company, suffered a loss of over \$300,000 as the result of one of its accident benefits claims adjusters intentionally processing payments for fraudulent invoices in claim files.

The adjuster had authority to approve invoices and issue payments to third party vendors who provided medical services to the company's insureds. Taking advantage of the information at her disposal, the adjuster colluded with outside parties to perpetrate the scheme. The claim's adjuster was able to avoid detection for over 3 years by ensuring that the file notes always reflected a legitimate payee, even when the cheques were made payable to the fraudulent vendors. The scheme was eventually discovered when an internal auditor noted that the adjuster was regularly issuing cheques to vendors that no other claims adjusters were issuing payments to, and that the medical services being billed did not match the patient treatment plans on file. Chubb provided coverage in the amount of \$175,000.

Insurance Company - Agent Fraud

Description of Event:

Our insured, an insurance company offering life, medical, and investment products, suffered losses of over \$2 million as the result of a premium rebating scheme perpetrated by one of its sales agent employees (the agent). The agent sold life insurance policies to individual clients, receiving upfront commissions on these sales from the insured. After several years of service, the agent began binding policies to actual client accounts without their knowledge and funded the premiums herself in order to collect the upfront commissions.

As a result of the rebating scheme, our insured suffered a direct loss based on the dishonest acts of its agent, as well as significant consequential losses. Chubb provided coverage in the amount of over \$2 million.

Bank - Cheque Kiting Scheme

Description of Event:

Our insured, a Financial Institution, suffered losses over a 10 year period as the result of a cheque kiting scheme perpetrated by a dishonest employee. The long-standing employee, had access to blank cheques for one of the company's clearing accounts. For years, he issued cheques for amounts between \$3,000 and \$15,000 payable to "cash" from the clearing account, which he then misappropriated. Taking advantage of his intimate knowledge of the process and payment schedules, the employee was able to shift deficits from one account to another in order to hide them on month-end reports. To mask the deficit from an accounting standpoint, he falsified daily deposit ledgers and recorded backdated reimbursements to hide the additional transactions. Chubb provided coverage in the amount of \$2 million.

Bank Acquired Subsidiary Loss

Description of Event:

Our insured, a bank, suffered a cheque kiting loss committed by an administrative manager of a recently acquired asset management firm. The thefts were committed both pre-acquisition and post-acquisition, and involved an employee falsifying reconciliation reports and account statements in order to steal funds from internal accounts. In order to mask the thefts, the employee would credit the accounts left in deficit by replenishing them with funds stolen from other accounts. The employee also fraudulently modified general ledger entries, and as a result, was able to covertly steal funds for a period of 10-15 years. In total the employee stole approximately \$3.5 million; net of deductible Chubb provided coverage in an amount of approximately \$3 million.

Asset Manager - Cyber Hedged Fraud

Description of Event:

Our insured, an asset management firm, shared a mutual client with a third party asset management firm (the "TPAM"). The TPAM had its email system compromised by an unknown attacker, which resulted in a fraudulent phishing email being sent from the TPAM to our insured. An employee of our insured clicked a link within the email and entered their username and password when prompted; this resulted in their email account being accessible to the attacker. Our insured quickly identified the breach and blocked further access within 48 hours. That said, two weeks later the attacker sent an email to a separate client of our insured (posing as their Portfolio Manager) using a spoof email address. The spoof email requested that the client transfer \$260,000 held in their account to a third party bank account. The client transferred the funds to the third party bank account, and upon realizing that it was a fraudulent request notified our insured. Our insured thereafter contacted a Chubb referred breach coach who helped guide the insured through a cyber-breach remediation. Working in concert with the breach coach, and a Chubb referred electronic forensic firm, our insured was provided with a thorough analysis of the incident and assurance that the breach had now been completely sealed off. This feedback further assisted our insured in strengthening their security systems. Chubb provided crisis management expense coverage under its *Cyber Hedged* enhancement coverage, for the breach coach and forensic firm in the amount of approximately \$50,000.

Chubb. Insured.SM