



Vendor Email Hacked

Coverage: Crime Insurance

Cause of action: Social Engineering Fraud

Type of organization: Private Company

Number of employees: Less than 250

Annual revenue: Less than \$250 million

The controller for a distributor of component parts was responsible for making regular payments to overseas vendors from which the distributor purchased products for resale in the United States. After many months of working with one particular vendor and receiving regular shipments, the controller received an email that appeared to come from his vendor contact, indicating that the vendor's bank was having issues with accepting payments, and asking if the next payment could be made to a new bank. Due to the vendor's overseas location, verification was a challenge. After the supposed vendor applied some pressure, the controller paid the invoice via wire transfer.

Resolution: The following month, when the real vendor realized that its best customer's payment was overdue, an investigation determined that the vendor's email had been hacked, and an imposter had been socially engineering the company into believing that the change in bank information was authentic. In the end, the fraudster finagled almost \$250,000 from the distributor.

Fake CEO Scam

Coverage: Crime Insurance

Cause of action: Social Engineering Fraud

Type of organization: Public Company

Number of employees: More than 250

Annual revenue: More than \$150 million

The regional CFO of a subsidiary of a large, publically traded company received an email purporting to be from the assistant to the CEO in the United States. The email requested that the CFO transfer a large sum of money immediately to facilitate covering a tax payment in China. When the CFO questioned the request, a follow-up phone call was made to the CFO, assuring him that the proper authority was granted and that it had come "from the highest levels" within the organization. With intimate knowledge of company policies, and an official looking letter on company letterhead "authorizing" the transfer, the CFO transferred the money by wire. The scam was detected after another attempt at transferring funds was stopped by the subsidiary's bank.

Resolution: After recovering only a portion of the original wire transfer, the subsidiary suffered a \$1 million loss.



Illegitimate Client

Coverage: Crime Insurance

Cause of action: Social Engineering Fraud

Type of organization: Private Company

Number of employees: Less than 50

Annual revenue: Less than \$100 million

A business manager handling bill payment and bookkeeping services for a client received an email, purportedly from a client, inquiring about her balance and availability of funds for a wire transfer. The email included details regarding the scope of services that were provided, as well as information about other transactions that had recently been performed. The wire, for \$100,000, was to go to an offshore account, purportedly for the purchase of a new piece of real estate. After the purported client won the business manager's trust, the business manager authorized wiring the funds to the fraudster's account.

Resolution: After noticing some activity in the client's spam account, the client grew suspicious and contacted its bank, requesting that the wire be stopped. Unfortunately, the wire had been sent and all \$100,000 was lost.

Something for Nothing?

Coverage: Crime Insurance

Cause of action: Social Engineering Fraud

Type of organization: Law Firm

Number of employees: Less than 200

Annual revenue: Less than \$100 million

A regional law firm received a request to sign up a new client from overseas. The new client wished the firm to pursue a debtor in the United States who was delinquent on its bills. The client explained that it would pay the retainer and entered into an agreement with the law firm. During the vetting process, the client informed the firm that the debtor had agreed to pay the bill, but had already written the check to the law firm. The client instructed the law firm to cash the official looking cashier's check that had just arrived, deduct its fee, and wire the remainder to the client.

Resolution: The check provisionally cleared the client's bank, but because of effective routing, the hold expired after the firm had already wired out the funds. The fraud was detected when the check bounced, and the fraudster was long gone. All \$250,000 was lost, as the wire could not be recalled.

To Learn More

Contact your Chubb Crime Insurance underwriter or visit us online.



Chubb Group of Insurance Companies | www.chubb.com

Loss scenarios are hypothetical in nature and for illustrative purposes only. Whether or not or to what extent a particular loss is covered depends on the facts and circumstances of the loss and the terms, conditions and endorsements of the policy as issued. It is impossible to state in the abstract whether the policy would necessarily provide coverage in any given situation. Consult your agent, broker or other expert.

Form 14-01-1140 (Ed. 7/14)