Crime Insurance and Fidelity Bonds Case Studies: U.S.

Companies across all industries, sizes, and locations are increasingly confronted by the risk of fraud and dishonesty in many forms, from an employee creating and issuing payments on fraudulent invoices, to spoof emails requesting payment to a fraudster's account, a contractor pilfering property from a client's premises, or a hacker forging account withdrawal forms.

The following case studies illustrate the benefits of comprehensive Crime Insurance and Fidelity Bonds coverage and an experienced carrier in responding to these risks.

Employee Theft

Employee Issues False Vendor Payments to Own Account

Industry: Manufacturing

Size: 500+ employees

During an accounting audit, a manufacturer insured discovered payments to an unauthorized vendor. All payments had been processed by the company's IT manager, who was unable to sufficiently answer questions related to the vendor, to the goods or services the vendor provided, or why payments to the vendor were not made using the preferred wire transfer or check methods. The manufacturer performed an initial investigation and discovered payments made to several companies with similar names and descriptions, none of which were an actual vendor. Suspecting fraud, the company reported the issue to AIG and triggered the Fidelity Research & Investigative Settlement Clause (FRISC) benefit of their AIG Crime policy. Under FRISC, AIG and the insured engaged a leading third-party forensic firm, which confirmed the fraudulent transactions and completed an exhaustive investigation to learn the full scope of loss. The investigation determined the IT manager falsified invoices using a generic company name then paid those invoices using his corporate credit card, directing the payments to an online account under his control. Initially, the payments were small but increased significantly over the five years of the fraud. The complex investigation uncovered a total loss of over $2 million, which the AIG policy fully covered.

Employee Purchases Office Supplies to Resell

Industry: Municipality

Size: 13,000+ employees

An employee of an insured municipality used his employee credit card to buy $1.4 million in printer toner, which he then transported to his home to resell online. He also used the card to make $21,000 in additional personal purchases from online retailers. The fraud went on for several years before the insured discovered discrepancies in its inventory. The insured performed accounting and inventory audits to determine the extent of the loss, and with proof of loss, the AIG policy promptly paid the $1 million policy limit.

Employee and Vendor Collude on Theft Scheme

Industry: Healthcare

Size: 100,000+ employees

While conducting an inventory audit, an insured hospital discovered a $5.6 million discrepancy in supplies. The hospital reviewed its purchase orders for the missing inventory and found that all the orders had been made by the same employee using a limited-use vendor after that vendor's authorization had ended. Further, the purchase records for the missing inventory did not include proof of delivery. The hospital's investigation uncovered that the employee had directed staff to validate receipt of items that were not actually received, and that the employee sold the items online and split the proceeds with the vendor. The AIG policy covered the full loss amount and AIG worked closely with the hospital to identify and implement improved purchasing and inventory control practices.

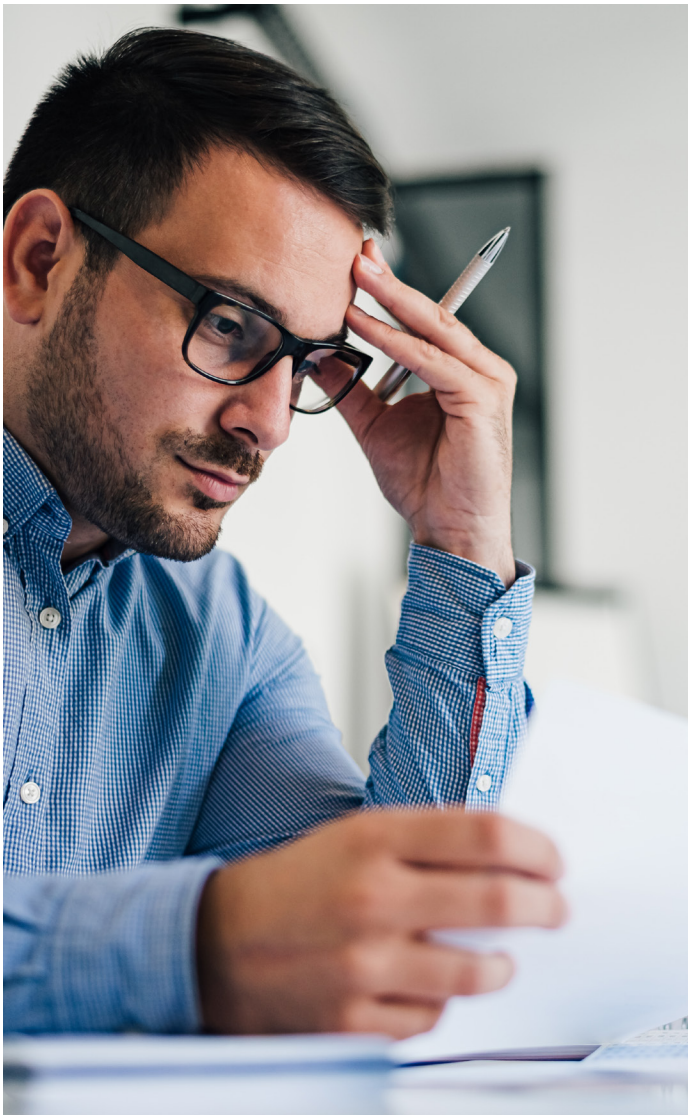
Computer Fraud

Phishing Email Results in Digital Gift Card Scheme

Industry: Wholesale/Retail

Size: 100+ employees

An employee of an insured wholesale digital gift card distributor fell victim to a phishing email, which allowed hackers access to the distributor's computer system. Once in the system, the hackers imitated the purchase of $2.9 million in gift cards from a retail business within the insured's network, which were activated at the time of the purchase, and began redeeming the cards before the insured discovered the fraudulent order. The insured immediately contacted the retail business, who was able to deactivate the unredeemed cards with approximately $1 million in value remaining. The fraud was reported to local and federal authorities, with whom AIG and the insured worked closely to investigate the events and the source. The loss ultimately amounted to $1.9 million, which was paid in full by the AIG policy.



Online Banking Credentials Stolen through Spoofed Website

Industry: Financial Services

Size: 9,000+ employees

Fraudsters duplicated an insured bank's website and used search engine optimization attacks to drive the bank's clients to the spoofed site. Clients, not realizing they were on a fake website, entered their online banking credentials to access their accounts. The credentials were tracked by the fraudsters, who then used them to transfer clients' funds to their own accounts. Clients who noticed unauthorized transfers from their accounts alerted the bank, and the authorities were promptly engaged. Dozens of accounts were impacted, with a total loss amounting to more than $1.5 million. AIG worked closely with the bank and local and federal authorities throughout the investigation and claim evaluation to ensure a smooth, efficient resolution. Accordingly, the loss was covered in full by the AIG policy.

Impersonation/Social Engineering Fraud

Funds Transferred to Fraudulent Account Unable to be Returned

Industry: Construction

Size: 40,000+ employees

An insured construction contractor centralized the administration of cash accounts of the contractor's project subsidiaries. Responding to a request apparently made by a subsidiary's managing director, the contractor transferred $900,000 of the subsidiary's funds to an external bank account. It was unknown at that time that the subsidiary had suffered an email hack, which allowed first a spoof email which appeared to be from the managing director to the insured requesting an update to payment accounts and then a second spoof email requesting the funds transfer. The fraud was quickly discovered, and the contractor attempted to recall the transfer; however, the receiving bank was unable to return the funds. The social engineering endorsement added to the AIG policy covered the full loss amount. AIG worked with the insured to identify and analyze the weaknesses in its internal procedures that had enabled the fraud and recommended new controls and best practices to reduce the likelihood of recurrence.

On Premises

Employees Steal Car Batteries in Broad Theft Ring

Industry: Transportation

Size: 5,000+ employees

An insured transportation company reported to the police the theft of 15 pallets of used car batteries, which the company had been storing for a client in its warehouse. The company believed a former warehouse manager and dock contractor were involved, however there was insufficient evidence to make any arrest. Local authorities suspected the incident was tied to a larger theft ring involving other warehouses in the area, so the insured requested that its client, the owner of the batteries, verify its inventory. The client's investigation revealed additional missing batteries and ties to the suspect employee and contractor. Both men were ultimately charged with wire fraud, interstate transportation of stolen property, and money laundering. The indictment alleged that the men stole batteries from the insured, its client, and other warehousers to sell to local recycling businesses. The thieves pleaded guilty and were ordered to make restitution. Following the trial, the client made a claim against the insured for $1 million, the amount of the loss that was ultimately found to involve the client's batteries. The AIG policy covered the full loss less the restitution repaid by the thieves.

Forgery/Alteration

Withdrawal Form Forged by Fraudster

Industry: Financial Services

Size: 200+ employees

A fraudster hacked into the email system of an insured investment advisor's client. Impersonating the client in an email, the fraudster requested a funds withdrawal form, which the advisor supplied, believing it was communicating with its client. Using the hacked email, the fraudster completed the withdrawal form, requesting a $79,000 transfer, forging the client's signature, and returning the faked form to the advisor. When the client received her account statement showing the withdrawal, she notified the advisor that the transfer was fraudulent. The advisor immediately engaged local authorities and investigated the incident. The fraudsters could not be identified, and the funds could not be recovered. The AIG policy covered the full amount of the loss.

AIG is a leading provider of Crime Insurance and Fidelity Bonds for commercial organizations and financial institutions of all sizes. We have long specialized in bringing these vital solutions to small and midsize organizations. Our crime and fidelity underwriters, who average more than two decades of experience, tailor coverage for each client's unique needs. Our dedicated claims team and our underwriters continually track emerging loss trends and partner with insureds to ensure coverage and controls continually outpace evolving risks.

Contact

For more information, please contact your local Financial Lines underwriter or email FinancialLines@aig.com.

AIG

502-01-125US