CAMBRIDGE
PROPERTY & CASUALTY
SPECIAL REPORT

WE DON'T NEED FUNDS TRANSFER COVERAGE BECAUSE WE DON'T DO WIRE TRANSFERS, OR DO WE?

This Special Report was written by Daniel P. Hale, J.D., CPCU, ARM, CRM, LIC, AIC, AIS, API. Mr. Hale is Vice President of Cambridge Property & Casualty and an attorney licensed to practice law in the State of Michigan. He can be contacted at 734-525-2429 or dhale@cambridge-pc.com. More Special Reports are available at www.cambridge-pc.com.

What if one of your employees was fraudulently induced by a third party to change your banking passwords through an email scheme? The fraudulent email appeared to have been sent by your bank and was consistent with previous emails you had received. Assume that this then gave the third party access to your business and personal accounts and you were defrauded over one million dollars in business and personal funds held with the bank. Would your insurance policies cover the financial loss?

INTRODUCTION

No company is immune to crime losses. Mergers, acquisitions, downsizing, restructuring, rapid expansion, and globalization have increased the challenges of maintaining a strong system of internal controls. Likewise, the advancement of technology has drastically changed the speed with which fraud can occur. As a result, employee theft is on the rise. Even the best financial controls are not foolproof. A sophisticated criminal-minded employee may be nearly unstoppable and extremely difficult to spot.

With few exceptions, the standard property policy excludes or substantially limits coverage for most crime exposures such as employee theft, burglary, check fraud, computer fraud, funds transfer fraud, money order fraud, and credit card fraud. Even if your company maintains a separate crime policy, many coverages (such as for computer crimes) are optional and must be purchased separately.

The purpose of this Special Report is to review the basic elements of crime insurance as they relate to computer and electronic fraud.

FUNDS TRANSFER FRAUD

Funds transfer fraud coverage applies if a financial institution transfers money or securities based on fraudulent documentation purported to have been sent by your organization.

Funds Transfer Fraud means fraudulent written, electronic, telegraphic, cable, teletype or telephone instructions issued to a financial institution directing such institution to transfer, pay or deliver money or securities from any account maintained by an insured organization at such institution, without an insured organization's knowledge or consent.

For example, a criminal might send a fraudulent message to your financial institution directing them to transfer money to their account, such as the fraudulent email scheme discussed earlier.

COMPUTER FRAUD COVERAGE

In today's electronic world, the risk of sustaining a loss of money, securities, or property at the hands of a hacker has also increased substantially.

Most crime policies define computer fraud as the unlawful taking of money, securities or property resulting from an unauthorized entry into or deletion of data from a computer system; a change to data elements or program logic of a computer system, which is kept in machine readable format; or an introduction of instructions, programmatic or otherwise, which propagate themselves through a computer system directed solely against any insured organization.

For example, a criminal might hack directly into your organization's computer systems in order to steal property or money.

FORGERY OR ALTERATION COVERAGE

Forgery and alteration coverage applies to forgery or alteration of a financial instrument, such as a check or draft issued by your company.

Most crime policies define forgery as the signing of another natural person's name with the intent to deceive, but does not mean a signature that includes one's own name, with or without authority, in any capacity for any purpose. Mechanically or electronically produced or reproduced signatures are usually treated the same as handwritten signatures. For example, a criminal might steal one of your checks from the mail and alter the payee information in order to steal funds.

OTHER CRIME COVERAGE

In addition to the above, crime policies also offer a host of other coverages such as employee theft, premises theft, in-transit theft, money order fraud, counterfeit currency fraud, credit card fraud, fraud expense coverage, and coverage for third parties, such as customers and clients. Note that some of these coverages are optional and therefore not included automatically.

- **Employee theft coverage -** Losses of money, property or securities that have been embezzled by *an employee* through acts of theft or forgery.

- **Premises coverage** - Losses of money, property or securities that are unlawfully taken, destroyed, or disappear from our customer's premises. Insurance also extends to property lost in a robbery or safe burglary that occurs on premises.

- **Transit coverage** - Losses of money, property or securities that are unlawfully taken, destroyed, or disappear while being transported or as the result of a robbery that occurs during transit.

- **Forgery coverage** - Losses resulting from forgery or alteration of a financial instrument, such as a check or draft issued by your company.

- **Computer fraud -** In today's electronic world, the risk of sustaining a loss of money, securities, or property, such as inventory, at the hands of a hacker has increased substantially.

- **Funds transfer fraud coverage -** Provides insurance if a financial institution transfers money or securities based on fraudulent documentation purported to have been sent by your organization.

- **Client coverage -** Provides insurance against loss of money, securities, or other property for which the insured is legally liable or that it holds in any capacity.

- **Credit card fraud coverage** - Provides insurance against the alteration of any written instrument required in connection with a credit card issued to the insured organization.

- **Money order and counterfeit currency coverage -** Protects against the good faith acceptance of a counterfeit money order or currency.

- **Investigative costs coverage** - Insurance which covers the cost of establishing the full extent of the loss.

MANAGING THE RISK

Some of the recommended prevention measures to workplace crime include:

- Having separate employees responsible for authorizing transactions, collecting or paying cash and maintaining records of accountability

- Safeguard storage facilities, including access to computers

- Conducting background checks on new employees

- Conducting regular fraud audits

- Establishing a fraud policy and prosecuting employees who are caught

- Requiring ethics training for all employees

- Having an anonymous fraud-reporting mechanism

- Installing workplace surveillance procedures (especially where assets are most vulnerable)

- Requiring every employee to take an annual vacation, during which someone else takes over his or her duties

CONCLUSION

The cost of computer fraud could cripple an organization. When you consider that more than a third of private companies have experienced a crime loss in the past five years, it is surprising that more do not purchase crime insurance. Purchasing schemes involving kickbacks, accounts payable fraud involving ghost vendors, payroll and check fraud, or inventory theft can reduce corporate profits by millions of dollars. We recommend that all organizations maintain some form of crime insurance consistent with their exposure.