September 26-29, 2024 I Sheraton Boston Hotel

09/28/2024
Insuring Cyber Crime
10:00 AM - 11:00 AM
Catherine Trischan
1 CEU

Sponsored by The Andover Companies

Insuring Cyber Crime

Catherine Trischan, CPCU, CIC, CRM, ARM, AU, AAI, CRIS, MLIS, TRIP, CBIA
catherine.trischan@gmail.com

Cyber Crimes

- Computer and Funds Transfer Fraud/Wire Transfer Fraud
- Business Email Compromise/Social Engineering/Fraudulent Impersonation/Invoice Manipulation
- Utilities Fraud/Telephone Toll Fraud/Toll Charge Fraud/Cryptojacking
- Ransomware/Cyber Extortion

Computer and Funds Transfer Fraud/Wire Transfer Fraud

- In these schemes, a criminal directs funds from the victim's accounts to its own account.
- The cybercriminal may access the victim's computer system to transfer money to its own account.
- Alternately, the criminal may directly access the victim's bank account, usually with stolen credentials, to transfer the money.

Computer and Funds Transfer Fraud Crime Coverage

CR 00 21 06 22/CR 00 20 06 22

First type of covered crime

- A thief enters or changes data within the computer system of the insured or that of a third-party performing services for the insured.
- The computer system in question may also be an employee's if the employee has agreed in writing to the insured's personal device use policy.
- This action by the thief must cause money, securities, or other property to be transferred to another or the insured's account at a financial institution to be debited or deleted.

Computer and Funds Transfer Fraud
Crime Coverage

CR 00 21 06 22/CR 00 20 06 22

Second type of covered crime

- A fraudulent transfer instruction is sent to a financial institution directing the financial institution to transfer money or securities from the insured's account.
- The fraudulent transfer instruction is by someone impersonating the insured.

Computer and Funds Transfer Fraud
Cyber Coverage

Sample Cyber Language
Computer and Funds Transfer Fraud

We will pay for Your loss of Funds resulting directly from a Fraudulent Electronic Instruction directing a Financial Institution to transfer, pay or deliver Funds from Your Account which is discovered during the Policy Period and noticed to Us as set forth in this endorsement.

Fraudulent Electronic Instruction means an instruction which purports to have been electronically transmitted, submitted, or approved by You, but which was in fact fraudulently transmitted, submitted or approved by someone else without Your knowledge or consent.

Computer and Funds Transfer Fraud
Cyber Coverage

Sample Cyber Language
Electronic Crime

*To indemnify the **Insured Organization** for the loss of **Money** or **Securities**, in excess of the **Retention**, contained in a **Transfer Account** at a **Financial Institution** resulting directly from **Funds Transfer Fraud** committed solely by a **Third Party**…….*

***Funds Transfer Fraud** means fraudulent written, electronic, telegraphic, cable, teletype or telephone instructions by a **Third Party** issued to a **Financial Institution** directing such institution to transfer, pay or deliver **Money** or **Securities** from any account maintained by the **Insured Organization** at such institution, without the **Insured Organization's** knowledge or consent.*

Note: One of the exclusions removes coverage if the sender ever had access to the Insured Organization's password, PIN or other security code.

Computer and Funds Transfer Fraud
Cyber Coverage

Sample Cyber Language
Funds Transfer Fraud

We agree to reimburse you for loss first discovered by you during the period of the policy as a direct result of any third party committing:

a. Any unauthorized electronic funds transfer;
b. Theft of money or other financial assets from your bank by electronic means;
c. Theft of money or other financial assets from your corporate credit cards by electronic means;
d. Any fraudulent manipulation of electronic documentation whilst stored on your computer systems; or
e. Any phishing, vishing or other social engineering attack against any employee or senior executive officer that results in the transfer of your funds to an unintended third party.

Business Email Compromise/Social Engineering/Fraudulent Impersonation

- BEC losses are often referred to as social engineering losses, although the term social engineering includes any type of crime that exploits human behavior.
- Spoofing and phishing are the starting points of this crime. A cybercriminal impersonates a customer, vendor, or someone within an organization.

Business Email Compromise/Social Engineering/Fraudulent Impersonation

- The thief sends an email to the organization's employee directing the employee to wire funds to a particular account. The employee, believing the instruction is a legitimate request, sends the money.
- A business receives a legitimate request for payment from a client or vendor. A criminal, impersonating the client, vendor or another employee of the business sends a request to change the payment instructions. The business, believing the change is legitimate, now sends or wires money to the criminal instead of to the client or vendor.

Fraudulent Impersonation Crime Coverage

CR 00 21 06 22/CR 00 20 06 22

First type of covered crime

- A legitimate instruction to transfer money or securities is sent to the insured by a client or vendor.
- Before the funds are sent, the transfer instructions are changed by the insured based on a fraudulent request by a criminal impersonating the client or vendor or someone in the insured's organization who has the authority to make such changes.
- The insured, following these instructions, unknowingly transfers money or securities to the thief.

Fraudulent Impersonation Crime Coverage

CR 00 21 06 22/CR 00 20 06 22

- **Second type of covered crime** - The insured transfers money or securities based on instructions from a thief impersonating a client, vendor, or another person within the insured's organization.

Fraudulent Impersonation
Crime Coverage

CR 00 21 06 22/CR 00 20 06 22

- The insured must make a reasonable effort to verify the authenticity of any change of account requests or transfer instructions in a way other than by email.
- Fraudulent Impersonation – Extended Coverage Endorsement (CR 04 18 06 22)
  - ➢ Extends coverage to other property in addition to money and securities

BEC/Social Engineering/Fraudulent Impersonation
Cyber Coverage

Sample Cyber Language

We will pay for Your loss of Funds resulting directly from Your having transferred, paid or delivered any Funds from Your Account as the direct result of an intentional misleading of Your employee, through a misrepresentation of a material fact ("Deceptive Transfer") which is:

- *relied upon by an employee, and*
- *sent via a telephone call, email, text, instant message, social media related*
- *communication, or any other electronic instruction…*
- *social engineering, pretexting, diversion, or other confidence scheme, and,*
- *sent by a person purporting to be an employee, customer, client or vendor; and,*
- *the authenticity of such transfer request is verified in accordance with Your internal procedures.*

Invoice Manipulation

- This crime begins with a business sending an invoice to its customer.
- Shortly after, a cybercriminal impersonating the business's employee contacts the customer and provides alternate wiring instructions. The customer unknowingly sends the funds to the criminal.
- Coverage is available under some cyber forms.

Utilities Fraud/Telephone Toll Fraud/Toll Fraud Charge/Cryptojacking

Telephone Toll Fraud

- In this crime, the cybercriminal accesses a business's Voice Over Internet Protocol (VOIP) system and uses it to make calls to expensive numbers.
- The business that was attacked gets a bill for the increased usage, while the criminal gets revenue from the calls made.

Crypto Mining/Cryptojacking

- A business's computing power is used to mine cryptocurrency without its knowledge.

Telephone Toll Fraud/Toll Charge Fraud Crime Coverage

CR 04 16 06 22 – TOLL CHARGE FRAUD

A. The following is added to Section **A. Insuring Agreements**:

Toll Charge Fraud

We will pay for loss from long distance telephone toll call charges incurred by you resulting directly from fraudulent use or fraudulent manipulation of an "account code" or "system password" required to gain access to your "voice computer system", provided such loss did not result from the failure to:

1. Install and maintain in operating condition a call disconnect feature to terminate a caller's access after three unsuccessful attempts to enter an "account code";
2. Incorporate a "system password"; or
3. Change a "system password" within the number of days shown in the Schedule.

…

Telephone Toll Fraud/Toll Charge Fraud Cyber Coverage

Sample Cyber Language

To indemnify the Insured Organization for any Telecommunications Fraud Loss, in excess of the application Retention…..

Telecommunications Fraud Loss means any direct financial loss to the Insured that results directly from a Third-Party gaining access to and using the Insured Organization's telephone system in an unauthorized manner….

Crypto Mining/Cryptojacking Cyber Coverage

Sample Cyber Language

Telephone Fraud means the unauthorized access to or use of an Organization's Telephone System from a remote location to gain access to outbound, long distance telephone service.

Computing Power Fraud means the unauthorized access to or use of an Organization's Computer System for the purpose of executing compute-intensive tasks, including but not limited to Cryptojacking.

Cloud Computing Power Fraud means the unauthorized access to or use of a Third-Party Service Provider's Computer System for the purpose of executing compute-intensive tasks, including but not limited to Cryptojacking.

Other Possible Crime Coverages Cyber Coverage

Sample Cyber Language
PHISHING COVERAGE

We agree to reimburse you in the event of fraudulent electronic communications or websites designed to impersonate you or any of your products first discovered by you during the period of the policy, for:

- *The cost of creating and issuing a specific press release or establishing a specific website to advise your customers and prospective customers of the fraudulent communications and*
- *The cost of reimbursing your existing customers for their financial loss arising directly from the fraudulent communications*
- *Your direct loss of profits for 90 days following your discovery of the fraudulent communications as a direct result of the fraudulent communications and*
- *External costs associated with the removal of websites designed to impersonate you*

Ransomware

- Malware that prevents users from accessing their system or files and demands ransom payment in order to regain access.
- The extortionist may also threaten to:
  - Release public details of the security breach and inform the media
  - Sell stolen information
  - Tell any stock exchanges about the hack and the loss of sensitive information
  - Use stolen information to attack clients and partners
- Double Extortion
  - 1st ransom demand – to decrypt the data
  - 2nd ransom demand – to delete the stolen data

Change Healthcare
(Parent Company as of 10/22 is United Healthcare)

- Attack began on 2/21/24. Technicians took the system offline to contain the attack.
- Cybercriminals used compromised credentials to remotely access a portal that allowed remote access to desktops. The portal did not have multi-factor authentication.
- Ransom Paid - $22,000,000 to AlphV/BlackCat – in exchange for a decryption key and a promise not to leak the company's stolen data
- A second ransomware group (RansomHub) claimed to have the stolen data and threatened to sell the data.
- Total loss is $1 billion +
- Clinics, hospitals and pharmacies couldn't properly bill, manage, and issue prescriptions and medical procedures. A survey of American Medical Association members conducted between 3/26 and 4/3 found that 4 out of 5 clinicians lost revenue as a result.
- United Healthcare didn't carry cyber coverage – spends $300 million per year on cybersecurity

Ransomware/Cyber Extortion Coverage

- Payments to a third-party related to a ransomware/extortion demand
  - May be money or virtual currency (e.g. Bitcoin)
- Reasonable and necessary expenses incurred to respond to the extortion threat

Cyber Extortion

Sample Language – Cyber Coverage Trigger

Network Extortion Threat means any credible threat or series of related threats directed at an Insured to:

- *release, divulge, disseminate, destroy, or use Protected Information, or confidential corporate information of an Insured, as a result of the unauthorized access to or unauthorized use of an Insured's Computer System or Shared Computer System;*
- *cause a Network Security Failure;*
- *alter, corrupt, damage, manipulate, misappropriate, encrypt, delete, or destroy Digital Data; or*
- *restrict or inhibit access to an Insured's Computer System or Shared Computer System,*

US Dept of Treasury
Office of Foreign Assets Control (OFAC)

The U.S. government strongly discourages all private companies and citizens from paying ransom or extortion demands and recommends focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks.

Facilitating Ransomware Payments on Behalf of a Victim May Violate OFAC Regulations

Under the authority of the International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA), 12 U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities ("persons") on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria). Additionally, any transaction that causes a violation under IEEPA, including a transaction by a non-U.S. person that causes a U.S. person to violate any IEEPA-based sanctions prohibitions, is also prohibited. U.S. persons, wherever located, are also generally prohibited from facilitating actions of non-U.S. persons that could not be directly performed by U.S. persons due to U.S. sanctions regulations.

US Dept of Treasury
Office of Foreign Assets Control (OFAC)

OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC.

Latest advisory is dated 9/21/2021

Ransomware/Extortion
Other Cyber Coverages

Breach response costs – e.g.

- Cyber forensics
- Legal analysis
- Notification costs
- Credit monitoring
- Call center

Crisis management/public relations

- Helps with the financial impact of adverse media

Ransomware/Extortion
Other Cyber Coverages

Data restoration

- Costs to restore, recover or replicate data that is damaged by a technology breach

Computer replacement/bricking

- Hardware and software that must be replaced

Business Interruption

- Business income loss and extra expenses resulting from interruption or failure of a computer system

Ransomware/Extortion
Other Cyber Coverages

Security Breach Liability
- Third party claims

Regulatory Defense and Penalties
- Legal liability for failure to comply with security/privacy laws

Insuring Cyber Crime - Considerations

- Crime and cyber forms vary widely among insurers. Different coverages are offered, and different names are used to identify the coverages. It is important to carefully review the details of the coverage being provided before deciding on a policy.
- It is important to make sure that, to the extent possible, there are no gaps or overlaps if both crime and cyber coverages are in effect. Other insurance clauses in each policy can produce unexpected results if both policies cover a particular claim.
- If both cyber and crime coverages are written with the same insurer, the claims process may be smoother if there are overlaps between the coverages.

Thank You for Being Here!

Catherine Trischan, CPCU, CIC, CRM, ARM, AU, AAI, CRIS, MLIS, TRIP, CBIA
catherine.trischan@gmail.com