Crime Insurance

and the COVID-19 Pandemic

April 2020

LOCKTON®

Heightened anxieties, remote working conditions and significant economic pressures are ideal conditions for those seeking to exploit and cash in on the impacts of the COVID-19 pandemic. While most people are practicing social distancing and limiting travel out of their homes, criminals are using this period as an opportunity to victimize people around the world.

The World Health Organization, Interpol, the United States Department of Justice, and a multitude of international, federal, state and local authorities have issued warnings about criminals preying on individual and business vulnerabilities during the global pandemic.

On April 8, 2020, the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency and the United Kingdom's National Cyber Security Centre reported COVID-19 is being exploited by malicious cyber actors. The joint alert advised that cybercriminals "rely on basic social engineering methods to entice a user to carry out a specific action … taking advantage of human traits such as curiosity and concern around the coronavirus pandemic" to click on links and open files. Techniques employed often attempt to create the impression of authenticity, so the recipient believes that it is coming from a trustworthy source.[1]

The FBI has noted the number of complaints received by its Internet Crime Complaint Center ("IC3") has mushroomed since the start of the pandemic. An FBI deputy director recently commented that, "[w]hereas [the IC3] might typically receive 1,000 complaints a day through their internet portal, they're now receiving something like 3,000-4,000 complaints a day," many of which are related to the pandemic.[2]

The U.S. Federal Trade Commission (FTC) advises fraudsters are tricking people by using COVID-19 messages. According to the FTC, "The FTC is getting a lot of reports about fraudulent calls, texts, and emails coming from people pretending to be from the Social Security Administration, IRS, Census, USCIS and the FDIC … These are all scams, and none of those messages come from a government agency."[3] Additionally, "Fear can cause normally scrupulous individuals to let their guard down and fall victim to social engineering scams, phishing scams, non-delivery scams, and auction fraud scams."[4] From January 1 to April 15, 2020, the FTC received over 18,000 reports of COVID-19-related scams, with loss in excess of $13 million.[5]

Potential claim sources

COVID-19-related working conditions and financial pressures may underly many crimes that may lead to a claim under a company's crime policy. Recent examples include:

- A financial institution received an email from a fraudster, posing as the CEO of a company who had previously scheduled a transfer of $1 million, requesting the transfer date be moved up and the recipient account be changed "due to the coronavirus outbreak and quarantine processes and precautions." The email address used by the fraudsters was almost identical to the CEO's actual email address with only one letter changed.[6]
- A bank customer was emailed by someone claiming to be one of the customer's clients in China. The purported client requested all invoice payments be changed to a different bank because their regular bank accounts were inaccessible due to "Corona Virus [sic] audits." The victim sent several wires to the new bank account for a significant loss before discovering the fraud.[7]
- A fraudster "usurping the identity of a legitimate company and advertis[ing] the fast delivery of FFP2 surgical masks and hand sanitisers[.]" The incident involved €6.6 million being transferred to an entity in Singapore for the purchase of the alcohol gels and face masks – the goods were never received.[8]
- German buyers were making an upfront payment of €1.5 million for face masks. Prior to the scheduled delivery date, the buyers were informed that the funds had not been received and that an emergency transfer of €880,000 was necessary – the face masks were never received. "It all started with an email address and website which appeared to be linked to a legitimate company in Spain selling face masks. Unbeknownst to the buyers, the site was a fake and their legitimate email addresses had been compromised."[9]

Underwriting considerations

Given the evolving working conditions necessitated as a result of the impacts of COVID-19, crime underwriters are paying particular attention to internal and external control processes, verification protocols for banking details and instructions, and employee training. In this regard, companies should be prepared to share with underwriters the following:

- If most or all staff are working remotely, details around IT security and secure network sign-on processes.
- Dual control and segregation of duties, if most or all employees are presently working remotely.
- Methods and means of call-back verifications in the event of a change in banking details.
- Emergency control measures that differ from the usual protocols used prior to COVID-19, including but not limited to treasury and AP controls, procurement, new supplier onboarding, IT and physical security measures.

Coverage implications

The crimes perpetrated by those taking advantage of the impacts of COVID-19 may raise significant coverage issues under crime and cyber policies.

Crime policies are typically designed to cover employee dishonesty, theft of money or securities within the insured's premises or while in transit, forgeries by third parties, and certain cybercrimes. Crime policies cover an insured's first-party losses resulting from covered events - they do not typically cover the insured's liability to third parties arising from those covered events. Critically, crime policies only cover actual out-of-pocket loss. They don't cover lost profits or business interruption loss.

One potential crime policy coverage question is whether losses incurred through the remote employee's personal laptop, when used for remote work, would be covered under the crime policy. The language of the particular crime policy at issue will govern, as to whether the remote employee's personal device is considered part of the insured's "computer systems." However, even where a company may not own the remote employee's computer, a crime policy may cover the loss as the company's "computer systems" because the computer is arguably operated and/or utilized by the company.

Another question centers around coverage for social engineering fraud crimes perpetrated using the COVID-19 crisis as the catalyst. Standard crime policies typically include coverage for computer fraud and funds transfer fraud. Computer fraud covers the insured's direct monetary loss resulting from an unauthorized entry into the insured's computer system (e.g., deploying malware to take the insured's funds). Funds transfer fraud covers the insured's loss of money resulting from a fraudulent transfer made without the insured's knowledge or consent (e.g., as a result of fraudulent instructions to the insured's banking institution).

Computer fraud insuring agreements usually require a "computer violation" to trigger the insuring agreement. A computer violation may be defined as an unauthorized entry into or deletion of data from a computer system committed by a third party. When social engineering claims are evaluated under the computer fraud coverage, insurers often conclude that there was no unauthorized entry into the insured's computer systems, i.e., there was an unsuspecting intermediary, who authorized the cybercriminal's access to the computer system. In other words, the entry into the insured's computer system was not "unauthorized" as required by the insuring agreement.

Similarly, insurers may deny coverage for COVID-19-related social engineering crimes under funds transfer fraud insuring agreements, reasoning that a transfer request made under an erroneous belief is nonetheless initiated with the knowledge and consent of the insured. Funds transfer fraud coverage is frequently triggered by a fraudulent instruction issued by the cybercriminal to the insured's banking institution directing a funds transfer, without the insured's knowledge or consent. When a fraudulent transfer is precipitated by social engineering, insurers have the opportunity to conclude that the lack of the insured's knowledge and consent elements are absent, i.e., the funds transfer was initiated by the insured and presumably with its knowledge and consent, notwithstanding the fact that it was tricked into making the funds transfer.

In addition to insuring agreement challenges for social engineering claims, crime policies often contain "voluntary parting" exclusions which preclude coverage for losses resulting from anyone acting on the insured's authority to voluntarily part with the company's money. Many social engineering claims causing monetary loss are occasioned by employees' misconceptions of a fraudster, combined with their intent on doing their jobs and trying to be helpful. Insurers may rely on this exclusion to deny coverage for social engineering claims reasoning that the loss was a voluntary parting, even if it was caused by a mistaken belief.

Recognizing these challenges, many crime policies now explicitly provide coverage for social engineering fraud, but the limits of that coverage may be lower than the full limits of the crime policy. Additionally, court decisions reveal a lack of clarity on the question of whether social engineering claims trigger the computer fraud and/or funds transfer fraud insuring agreements of crime policies. Some recent court decisions have found coverage under crime policies for social engineering claims.

A company's losses due to cybercrime may also trigger a cyber policy. Cyber policies cover various first-party losses, including data breach and system security failure expenses and potentially also business interruption losses, resulting from a covered cyber event. Some cyber policies provide coverage broad enough to address social engineering attacks, among other things.

Cyber policies also cover various claims made by third parties, including claims for breach of individual and corporate confidential information resulting from the cybercrime. As with crime policies, cyber policies often define the specific terms, such as employee, network and computer systems, and the same coverage implications and considerations relevant to crime policies are often relevant to cyber policies in the context of cybercrime.

To the extent a cybercrime potentially triggers both a crime and a cyber policy, it will be important to explore potentially available coverages under both policies to respond to these losses.

There are daily challenges presented by the unique circumstances of doing business during the COVID-19 pandemic. If your business has sustained or is at risk of sustaining a loss as a result of a COVID-19-related crime, we encourage you to contact us. Lockton has developed proprietary crime policies and cyber policies that can address some of the exposures arising from the COVID-19 pandemic. We will connect you with the appropriate Lockton team members to serve your needs.

Lockton's COVID-19 resources may be found at https://www.lockton.com/coronavirus.

Sources

[1] https://www.us-cert.gov/ncas/alerts/aa20-099a

[2] https://www.zdnet.com/article/fbi-says-cybercrime-reports-quadrupled-during-covid-19-pandemic/

[3] https://www.consumer.ftc.gov/blog/2020/04/scammers-are-using-covid-19-messages-scam-people

[4] https://www.secretservice.gov/data/press/releases/2020/20-MAR/Secret_Service_Coronavirus_Phishing_Alert.pdf

[5] https://www.consumer.ftc.gov/blog/2020/04/covid-19-scam-reports-numbers

[6] https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic

[7] Id.

[8] https://www.europol.europa.eu/newsroom/news/corona-crimes-suspect-behind-%E2%82%AC6-million-face-masks-and-hand-sanitisers-scam-arrested-thanks-to-international-police-cooperation

[9] https://www.interpol.int/News-and-Events/News/2020/Unmasked-International-COVID-19-fraud-exposed

UNCOMMONLY INDEPENDENT