RHSB
An Assurex Global Partner

CASE STUDY

North Texas ISD $2M Fraudulent Wire Transfer Event

December 18th, 2018 – The Star-Telegram released an article: "Florida man conned nearly $2 million from Crowley Independent School District in 2 Days". Read Full Article Here.

RHSB has evaluated this breach from an insurance perspective to educate you on coverage found in policies for this type of incident.

AT-A-GLANCE

The Who:

Industry: Public Education
A north Texas Independent School District

The What:

In 2018, a local ISD experienced a wire fraud breach which resulted in costing the District nearly $2,000,000.

The Why:

Evaluate similar potential breaches and provide guidance on how insurance coverage may respond under substantially similar circumstances.

Allison Nixon, ARM, CSRM
817.390.3519
anixon@rhsb.com

1320 S. University Drive, Suite 1000, Fort Worth, Texas 76107
8750 N. Central Expressway, Suite 500, Dallas, Texas 75231
817.332.1313 972.231.1300 800.295.6607 rhsb.com

THE FACTS AS REPORTED

- A Florida resident, Donald Howard Conkright, 61, has been charged for conning close to $2 million from Crowley Independent School District (CISD) in November of 2018.
- The Director of Accounting at Crowley ISD received an email from an accountant at what appeared to be a construction vendor, Steele & Freeman, Inc., that the District dealt with frequently. Subsequently, the District updated the banking information per the fraudulent request, which did not in fact come from the vendor.
- Initially, CISD sent a $1.00 payment to the updated account to ensure it worked. Once confirmed, they continued the payments.
- As a result of the alleged scam by Conkright, Crowley ISD lost $1,995,715.
- Once learning of the fraudulent activity, CISD notified authorities including the FBI and this investigation is still currently on-going.

Source: Star-Telegram

Disclaimer: RHSB has not worked with Crowley ISD on their insurance program. This RHSB evaluation is independent and based on the facts from local news publications and hypothetically evaluates how insurance coverage would respond in the event of a similar breach.

EVALUATION

1

Q: Where would a wire fraud breach that leads to a fraudulent transfer of funds be covered under insurance policies?

A: Both Crime policies and Cyber policies could respond to funds transfer fraud which is also referred to as social engineering. It is important to read through coverage forms carefully because oftentimes one policy is broader than the other. Because the coverage is available in both products, we typically see and recommend that insureds carry both products wherever they can since this coverage is typically sub-limited. This means one policy might respond in excess of the other if the claim exceeds one sublimit. For example, if the insured has $100k in Social Engineering on a Traveler's crime policy and $100k in a Lloyd's Cyber product then in the case that a social engineering event resulted in $150k funds lost, both policies would potentially respond.

2

Q: Are there differences/advantages in coverage for Social Engineering on a Cyber Policy vs. a Crime Policy?

A: Many would argue that a Cyber Policy is the best home for this coverage because it would trigger any other first party expenses that came about as a result (i.e having your systems inspected by computer forensic professionals). Therefore, higher limits are often requested on Cyber Policy placements.

There is a difference between what Social Engineering, Fraudulent Funds Transfer, Phishing, and Invoice Manipulation mean across Cybercrime language so you must be cautious to read your policy form closely.

In Crime policies, it would be important to read the carrier's Computer Fraud or Social Engineering wording carefully. Some crime carriers still put "Authentication Challenge" language in their coverage which means the insured would have to prove that they made an attempt to validate the funds transfer request by an alternative means of communication before executing it. In this example, if Crowley had this clause on their policy, the Director of Accounting would have had to call the vendor and verify that they made the request to update wire instructions. Otherwise, their rights to coverage would likely have been compromised or eliminated. RHSB recommends

trying to remove this restriction or placing coverage elsewhere if that authentication requirement is included because this can often render coverage useless. In almost any case, if the insured had made the attempt to authenticate by other means of communication, the claim probably would not have happened.

3

Q: Are there differences in coverage triggers resulting from Social Engineering Fraud on a Cyber Policy vs. a Crime Policy?

A: Some Cyber Policy crime language limits the coverage to where it can only trigger if there was a cyber "event." Meaning, there would have had to be a breach of the insured's systems that caused malicious activity in the email or accounting systems. This type of coverage is more likely to trigger if the fraudulent funds were transferred due to internal instruction; i.e. the CFO's email is hacked and they ask the accounting department to send funds for a purchase to a different account which was not the case for Crowley ISD.

Alternatively, when the vendor or client is the one being compromised (which is the case with Crowley), then the above coverage scenario likely wouldn't apply since it limits the event to insured's system being breached. It is likely in these type of scenarios that the vendor's (the construction company) email system was infiltrated and that is how the alleged con man was able to use the construction company's employee email to dupe the District. We have seen circumstances where the malicious actor has even been able to intrude and view emails of past invoices and communications to legitimize their fraudulent emails even further. In this kind of case, hypothetically Crowley ISD would have a case against the construction company to recoup lost funds since it was a result of their system vulnerability that the fraudulent emails were initiated. Crowley's attorneys would demand damages from the construction company and (hopefully) that company would have proper Cyber Coverage in place that would respond accordingly. In this sample scenario, the District's Cyber Policy would not respond.

There are some Cybercrime Polices that don't limit impersonation fraud to the breach of systems. Because sometimes malicious actors are able to write fictitious emails by just changing a number or letter in the address or even by calling accounting personnel, a few markets have addressed this. Phishing fraud that dupes insureds into sending money can happen without systems being breached. This could have been the case with Crowley ISD if the construction company proves that there was no system intrusion. However, the amount of Cyber carriers willing to write this currently are far and few between and most are only offering $50k sub-limits since it is difficult to underwrite.

RECOMMENDATIONS

1. Talk to your agent regarding your Cyber and Crime Policies to conduct a thorough evaluation of the coverage you currently have (or do not have).

2. Review your applications on your Crime and Cyber Policies to ensure you have completed information correctly. In the event that you have accidentally misrepresented information this could affect your coverage in the event of a claim.

3. Though we recommended removing the "Authentication Challenge" from the policy, we would highly recommend that you create internal procedures and authentication checks and balances to prevent Social Engineering events. This type of loss is becoming more and more common and occurs often in very sophisticated companies and organizations. Hackers are becoming increasingly intelligent to make if exceedingly more difficult to identify fraudulent activity. Therefore, having certain procedures in place could help further efforts to prevent future claims.

ABOUT RHSB

Local Roots. Global Reach.

RHSB is an independent insurance broker providing insurance solutions to companies, families, and individuals.

RHSB has been serving the North Texas area for over 70 years. We're also the North Texas Partner of Assurex Global, the world's largest privately-held risk management and insurance brokerage group. That means we're able to leverage the expertise of more than 20,000 experienced independent professionals on six continents in order to help you with your national and international insurance needs. Additionally, our ownership in Assurex Global gives us buying power and market influence that translates into better terms and pricing for all of our clients, not just the ones with global operations.

CONTACT INFO

Phone
972.231.1300

E-mail
anixon@rhsb.com

Website
rhsb.com

RHSB At-A-Glance:
Independently Owned. Worldwide Capabilities. Half a Century of Experience.

- Independently owned and managed
- Full-service offices in Dallas and Fort Worth
- Full range of services and coverages for both businesses and individuals
- Serving local, regional, and global companies in virtually every business sector
- Worldwide capabilities in 130 countries on six continents
- An Assurex Global partner, offering extensive access to insurance carriers and underwriters in world markets
- A TechAssure partner, providing deep expertise and specialty programs for the technology industry

ALLISON NIXON BIO

Allison Nixon, ARM, CSRM, Vice President, Principal

Allison Nixon is a sales executive focusing on Property & Casualty. She is also Team Leader of the Public Entities team providing insurance solutions in the role of broker or consultant for many large public entities, including municipalities, public schools, large community colleges, and non-profits. Allison has a sales background and is known for building strong relationships because of her passion for people. She has experience managing and growing sales teams, creating marketing and branding strategies with a focus on solutions. Allison is a graduate of Texas Christian University with a degree in International Advertising and Public Relations.

Professional Designations/Licensing/Education

Certified School Risk Manager
Associate in Risk Management
Licensed General Lines Agent-Life, Accident, Health and HMO, Property & Casualty Texas
Bachelor of Arts degree in International Advertising/Public Relations from Texas Christian University