Lowenstein Sandler

Insurance Recovery

February 27, 2023

Call Me, Maybe? The Stealth Disappearance of Social Engineering and Fraudulent Instruction Coverage

By Lynda A. Bennett and Richard F. "Trip" Connors III

Anyone who owns a cellphone or uses an email address has received a communication from a scammer seeking to extract confidential information or trick the recipient into sending money to foreign countries. These attempts come in a variety of forms that have evolved, and have become more sophisticated, over time. In the early days, it was a random email request to send money to the king of Zimbabwe, then it was the "internal" email from a high-ranking member of the organization asking for the purchase of gift cards or urgent late Friday afternoon wire transfer requests, and now the scammers have really upped their game by accessing systems to change payment instructions through the use of spoofed emails to reroute payment of ordinary course-of-business expenses to phantom foreign bank accounts.

As recently as three or four years ago, there was explicit insurance coverage for these types of social engineering and fraudulent instruction claims, and full policy limit protection was often offered–sometimes under a crime policy, other times under a stand-alone cyber policy, and maybe even both policies were available. However, as these types of claims began to proliferate across every industry of every size and geography, insurers started to pump the brakes on the scope of coverage provided. Initially, the pullback was accomplished through the use of sub-limits, meaning that insurers were still willing to provide coverage for social engineering and fraudulent instruction claims, but they would not agree to pay up to the full policy limit for them. Instead, insurers placed sub-limits–typically in the range of $100,000 to $250,000–on coverage for those claims.

Because scammers have remained dogged in their efforts to steal money and continue to have success across businesses of all types, sizes, and geographies, the insurance industry is taking a new approach to curtailing the level of insurance coverage protection that is available for these types of claims. The approach is concerning because insurers are not being forthright about the disappearance of the coverage but rather have quietly added policy language that, in essence, makes it incredibly challenging, and in some instances impossible, to secure any actual recovery for the claim.

If insurers wanted to be direct about the fact that they no longer will agree to insure social engineering and fraudulent instruction claims, they would put a clear and unambiguous exclusion in the policies and reduce the premiums charged for those policies to be commensurate with the reduction in coverage. But the insurers have chosen a more clandestine route, which appears to be designed to allow them to have their cake and eat it too. Most policy forms continue to offer, and charge premiums for, social engineering/fraudulent instruction coverage, but now, to access that coverage, a policyholder must "independently verify" a change in payment instruction before sending money to the vendor or other third party. Indeed, some policies go so far as to state that the "independent verification" must be accomplished using a communication method ***other than*** the method of communication used to make the change in electronic transfer or payment.

In other words, insurers are requiring policyholders to pick up the phone and call the sender of the email seeking to change the payment instructions to confirm that the request is not a scam before actually making the change and eventual payment. Of course, in our digital society, telephone calls have gone the way of the dodo bird, and the very reason that social engineering and fraudulent instruction scams succeed is because our workforce is accustomed to (and sometimes trained to) work "seamlessly" over email and ***not*** communicate over telephone lines.

So what are the lessons here?

First, as a best-practice risk management tool, companies must train (and remain vigilant in training) personnel who are responsible for the movement of electronic payments in or outside the organization to follow Carly Rae Jepsen's sage advice: Do not make any change to wire or payment instructions without first speaking to a ***live human being*** to confirm the requested change. And bear in mind that these scammers are good; even if your employee sends a ***separate email*** to the scammer asking for "proof" of the instruction change, the company may still be facing a coverage dispute with its insurer, depending on the wording of the insurance policy, because sending another email (likely to the same fraudulent address) may not be deemed a different form of communication for verification purposes.

Second, that last point segues into a crucial theme that overrides all insurance coverage claims and disputes: ***The words of the insurance policy always matter.*** Therefore, before accepting a knee-jerk denial of coverage on a social engineering/fraudulent instruction claim, companies will be well served to review with experienced coverage counsel their insurance policy language and insurer coverage position letters to determine whether coverage exists based on the facts of the claim.

Finally, because the policy words always matter, it is also crucial for policyholders to pay careful attention to the renewal of their crime and cyber liability insurance policies. Insurers will continue to tinker with and refine insurance policy language year over year as cyber claims activity continues to remain high, losses continue to stack up, and insurers look for ways to level the amount of dollars they will have to incur paying claims. Here too, experienced coverage counsel can provide important insights into current claim trends and what the "market standard" is in terms of policy wording for this significant risk category.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

LYNDA A. BENNETT
Partner
Chair, Insurance Recovery
T: 973.597.6338
lbennett@lowenstein.com

RICHARD F. "TRIP" CONNORS III
Associate
T: 862.926.6574
rconnors@lowenstein.com