Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Key Strategies For Insuring Social Engineering Risks

By **Matthew Schlesinger and Scott Levitt**

Law360, New York (August 1, 2017, 2:38 PM EDT) -- While scams to trick people to part with money or information may be as old as humankind, the sheer amount of information now publicly available online has facilitated and emboldened criminals who use that information to impersonate an employee, vendor or customer fraudulently directing a company's employee to transfer funds. These schemes go by various names such as social engineering fraud, fake president fraud or business email compromise. This article provides guidance from policyholder counsel about how to maximize the prospects that insurance will be available to cover losses resulting from such schemes.

Matthew Schlesinger

Scott Levitt

Coverage Specifically Written to Insure Social Engineering Risks

This coverage, sometimes called fraudulent impersonation or social engineering fraud coverage, may be available as an add-on (usually for an additional premium) to crime, fidelity and cyber policies. Currently, social engineering coverage often is subject to low dollar sublimits likely insufficient to cover a loss of any significant size. In any event, policyholders considering or purchasing such coverage should be aware of potential pitfalls and how best to avoid them.

Some social engineering endorsements exclude coverage if the policyholder's employee failed to require that the requestor of the funds transfer authenticate the transaction using a different method from that used to make the initial request, or to authenticate the transaction by using a method of "challenge and response." These hurdles, while they may be sound business practices for insureds to adopt, make the coverage less valuable to protect against the significant risk of employee negligence: i.e., that the insured's employee, failing to follow corporate policy, will unwittingly aid the fraudulent transfer of funds.

Another pitfall found in some express social engineering coverages is that the fraudster must be impersonating someone with a particular status, such as an existing employee. Some forms may permit the imposter to be the insured's vendor or client, with those terms often having a narrow defined meaning. For example, one form requires that the vendor be a "person or entity that provides goods or services to the [policyholder] pursuant to a written contract." A fraudster posing as a fictitious vendor, or one that does not have a written contract with the insured, would not qualify under such a policy.

The most protective type of policy will provide coverage if the imposter pretends to be an employee, customer, vendor or other third party, whether real or fictitious.

As with any insurance policy, conditions and exclusions may limit or preclude coverage. Those terms should be read with potential social engineering scenarios in mind. For example, insurers might argue that an exclusion for dishonest acts of an employee — unless covered under a different employee dishonesty insuring agreement — bars coverage if an employee somehow knowingly assisted a third party's impersonation, perhaps through something as simple as providing the name of someone in the insured's finance department to someone he or she knows engages in fraud.

Coverage for Social Engineering Risks Under Standard Crime Insuring Agreements.

Standard crime coverages for funds transfer fraud and computer crime (or the like) may be applicable to social engineering fraud, though some policy language is more restrictive than others. For example, the Insurance Service Office (ISO) coverage for a "fraudulent instruction," found in an endorsement titled, "Computer Fraud And Funds Transfer Fraud," includes a written or oral instruction "initially received by [the policyholder] which purports to have been transmitted by an employee but which was in fact fraudulently transmitted by someone else without your or the employee's knowledge or consent." A policyholder would argue that a written or oral instruction from an imposter posing as the insured's employee, which causes the policyholder's real employee to transfer funds, satisfies this definition.

Similarly, a typical definition of "Computer Fraud" may also be applicable to social engineering fraud, in that it covers "[t]he use of any computer to fraudulently cause a transfer of Money, Securities or Other Property" from the insured's financial institution. An insured would argue, for example, that an email directing the insured to transfer funds to a particular account satisfies the definition.

To be sure, policyholders pursuing coverage for social engineering fraud have encountered sharp resistance from insurers, with mixed results from the courts. Most recently, the U.S. District Court for the Southern District of New York ruled in Medidata Solutions Inc. v. Federal Insurance Co., No. 15-CV-907 (ALC) (S.D.N.Y. July 21, 2017), that a policyholder was entitled to coverage under a Chubb crime policy's computer fraud section, where a fraudster used "spoofed" emails to trick the insured's employees into wiring money overseas. These decisions are instructive about which policy language causes the most problems for policyholders.

Authority Exclusions

Some policies contain an exclusion for damages resulting directly or indirectly from the input of electronic data by an individual who has the authority to enter data into the insured's computer system. Alternatively, the policy may affirmatively require that the fraudulent entry of data or the funds transfer be "unauthorized." Insurers contend there is no coverage where an authorized employee sets in motion a funds transfer, even if induced by a fraudster. To avoid these arguments, policyholders should consider requesting during the renewal process (when the policyholder has the most leverage) that these exclusions be deleted or modified, or otherwise consider placement with an insurer whose standard form does not contain such language.

Requirement that Loss Arise "Directly" from Fraudulent Entry of Data

Insurers argue that a requirement that a loss arise "directly" from computer fraud or a fraudulent transfer instruction is not satisfied where there is an intervening act between the fraudster's action and

the transfer of funds — namely the activity of an employee of the insured who processes the transfer. Also watch out for the use of "indirectly" in exclusions. Insureds should inquire whether their insurers will delete the "directly" or "indirectly" limitations, and, if not, consider whether another insurer provides broader coverage for a comparable premium.

Transfers Required Without "Knowledge" or "Consent" of Insured

Insurers may seize upon a policy requirement that a transfer be without the insured's knowledge or consent to preclude coverage where the insured's employee knew about and effected a transfer of funds to a fraudster. Again, policyholders would be wise to request changes during renewal and shop around for insurers that offer more favorable language.

Along with innumerable advances for society, the cyber age has enabled criminals across the globe to target companies with as little effort as a few keystrokes and the click of a mouse. With some diligence, however, policyholders can ensure they have coverage that will protect them from cybercrimes such as social engineering fraud.

Matthew J. Schlesinger is a partner and Scott J. Levitt is special counsel with Covington & Burling LLP in Washington, D.C.