Insurance Coverage for Email Scams

By **PETER SELVIN**

A genuine looking email is sent to a company's accounts payable department with instructions from its president to pay money to a certain account. The "To" and "From" headers and the signature block look identical to hundreds of emails previously received by the department from the company's president. In reliance on the email, money is wired to the designated account. It later turns out the email was fake and the company's money was wired to a fraudster's account.

In another scenario, the company's accounts payable department receives an email purportedly from a trusted vendor. The email looks genuine, even down to the vendor's logo. In the email, the vendor states that it has changed its bank account and directs the company to make future payments to its new account. The company wires the money to the new account and later discovers that the money didn't go the vendor. It went instead to a fraudster who had impersonated the vendor.

Both of these scenarios fall under the category of "email spoofing", which refers to a form of cyber attack in which a hacker sends an email that has been manipulated to seem as if it originated from a trusted source. Otherwise known as business email compromise this technique is used

BACK TO CONTENTS

to dupe employees into moving money into a fake account.

According to the FBI, $43 billion in losses were sustained due to business email compromise between 2016 and 2021. This is a growing type of cybercrime that generates billions in losses every year. Companies that have been defrauded by these schemes ought to look at their crime policies, which typically have some or all of the following coverage grants:

Social engineering coverage. Many crime policies cover losses arising from so-called social engineering, which means the intentional misleading of someone within the insured company by someone impersonating a vendor or executive at the company. The challenge with this form of coverage is that losses are often subject to a lower limit (a "sublimit") than the other forms of coverage in a crime policy.

Companies that have been defrauded by business email compromise ought to look at their crime policies.

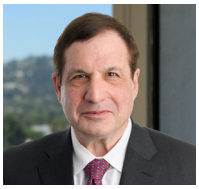
Computer fraud coverage. Particular attention should be paid to how a policy's computer fraud coverage is defined. Some policies require that there be a "fraudulent entry of data into a computer system and change to data elements or program logic of a computer system." This requirement may be met for losses arising from the first scenario – i.e., where a subordinate wires money in reliance on an authentic looking email from a corporate officer. In this regard, court cases have held that a third party's entry into and manipulation of a company's email system, in order to generate a genuine looking email, will be covered under this formulation.

Other policies define computer fraud in broader language. These policies cover losses arising from the use of a computer to fraudulently cause the transfer of funds from the company to a person or entity outside the company. This wording would cover losses arising from the second scenario – i.e., where the company sends funds in reliance on a genuine looking email purportedly from a vendor.

Funds transfer coverage. This is a narrower form of coverage. It covers losses from fraudulent instructions that are transmitted in the insured's name to a financial institution directing that the insured's funds be transferred to an outside account. Unlike the two scenarios above, this form of coverage typically does not cover transfers initiated by the company's instructions to a financial institution, even if that instruction was fraudulently procured by a third party.

Forgery coverage. This covers losses arising from the forged signature of an authorized signator on a financial instrument such as checks, drafts and promissory notes. Coverage under the forgery grant for losses arising from the two scenarios above is unlikely, although there is at least one case which has held that a fake instruction from a company's president, as used in the first scenario, may trigger coverage under this grant.

The take-away is very simple. Financial losses arising from this kind of email fraud may in fact be covered under a company's crime policy, but policy wording is always key. And, given how widespread this kind of email fraud has become, companies ought to make sure that they have the right kind of insurance coverage to protect against these losses.



Peter Selvin is a partner with the Los Angeles firm of Ervin, Cohen & Jessup. He practices in the areas of commercial litigation and insurance coverage and recovery. **pselvin@ecjlaw.com**