

BUSINESS EMAIL SCAMS ON THE RISE

In an alert to businesses last month, the FBI indicated that business email scams have accounted for \$2.3 billion in losses since 2013 and such scams more than tripled in this past year alone. The alert went on to say that such frauds are becoming harder to detect because attackers, who once pretended to be executives directing subordinates to transfer money, are using new techniques, including malicious software to break into email systems and redirect payments and other wire transfers. A recent analysis of fraudulent transfers indicated that over 80% went to accounts in China and Hong Kong where it is very difficult for victims to recover their money according to the FBI, and similar criminal enterprises have been noted in Africa, Europe, and the Middle East.

Since this is such a fast evolving area of losses for business, the insurance environment for such claims is somewhat unsettled. Many businesses purchase electronic transfer coverage as part of their crime insurance, but do not realize that many insurers include “call back” requirements, by which the coverage is voided if the insured did not take certain precautions before initiating a wire transfer which they did not realize was fraudulent.

Simkiss & Block can help guide businesses through a review of their exposures in this area, and where protection may be found in their crime, property, or cyberliability policies. Contact us for a discussion of this or other areas of exposure.