Published on *The National Law Review* https://natlawreview.com

# Email Account Compromise – What Is It And How Can Your Business Protect Itself From It?

Article By:

Heather J. Macklin

Scamming, phishing, pharming, vishing — people in the business world are well aware that hackers and other fraudsters have developed a myriad of schemes designed to obtain sensitive personal information and money. Every year, these schemes cause businesses to suffer significant financial losses. The FBI estimates that in 2020 business email compromise ("BEC") and email account compromise ("EAC") schemes caused losses of $1.86 billion. To combat these schemes, companies spend thousands of dollars to secure their computer systems and train their employees to recognize and prevent fraudulent schemes from succeeding. But no matter the preventative steps taken by businesses, hackers and fraudsters manage to stay one step ahead with new, creative schemes.

A recent fraud that businesses have unfortunately experienced is EAC, where hackers gain access to and use legitimate business email accounts of vendors and service providers to direct customers to send money to unauthorized accounts. EAC affects businesses ranging from small to large and can occur in any industry, including financial institutions, real estate, contractors and law firms. In a typical EAC scenario, hackers gain access to a person's actual email account and are able to monitor the incoming and outgoing correspondence in order to learn business practices, customer information and payment terms. At an appropriate time, the hackers use the email account to send payment instructions to a customer who legitimately owes money to the purported author's company. The customer receiving the email has likely communicated with the company and its employees previously and, having no reason to suspect the hacking, follows the directions and sends payment (ranging from thousands to millions) to a fraudulent account. By the time everyone realizes what has happened, the hackers and the money are long gone.

Because EAC is a relatively new fraud phenomenon, very few courts have had the chance to consider and decide the issue of who amongst the affected parties will ultimately bear the loss. Published legal decisions suggest that courts are tending to place liability on the party who was, in a given factual scenario, better able to prevent the fraud.

As governing legal doctrines are established, however, businesses are left to figure out how best to protect themselves from EAC and the resulting losses. Thankfully, numerous means of protection from EAC schemes are available. Three of the easiest are: (1) documentation, (2) communication and (3) insurance.

## Documentation

Prior to doing business with each other, vendors and their customers should memorialize the terms of their relationship in written contracts. In addition to the typical terms one expects to see in contracts (e.g., scope of work, agreed upon price and timelines, etc.), authorized payment methods and allocation of risk should be included. By agreeing up front as to how and where payments are to be made, the parties can ensure that any potential future EAC communications regarding payment will be immediately flagged and investigated. Moreover, by delineating who bears the risk of loss, should computer systems be *compromised* and payments be diverted, the parties will understand the duties and obligations they owe to one another and will hopefully take the steps necessary to protect their systems.

## Communication

When payments are owed and transfer of money between businesses is necessary, any emails received that contain directions for payments to be made to specific accounts or by certain methods should be verified prior to release of funds. The employee responsible for initiating the transfer of funds should not simply trust the email, even when it appears to have been sent from a legitimate and verified email account. Instead, they should personally reach out to the person who supposedly sent the email, either in person or via a telephone call, to confirm the directions are legitimate and the accounts actually belong to the company that is ultimately entitled to receive the payment. Only after successfully verifying authenticity of the payment instructions should the person initiate the fund transfer.

## Insurance

Businesses can and should obtain cyber-security insurance riders (which are not automatically part of standard business insurance policies) that provide coverage for losses caused by EAC and other information security breaches. Such policies provide an added layer of protection for companies when fraud is not timely discovered or prevented. All businesses should ask their insurance agents to confirm what cyber-security insurance options are available to them.

Although EAC and other information security fraud will unfortunately continue to plague the business world, companies can, by implementing these recommended practices, often prevent and/or protect against the significant consequences they might otherwise face.



National Law Review, Volume XII, Number 13