JONES DAY

ALERT

JUNE 2018

DOJ's Business Email Compromise Takedown Illustrates Pervasiveness of Internet Fraud Schemes

On June 12, 2018, the U.S. Department of Justice announced the internationally coordinated arrests of 74 individuals involved in a series of multimillion-dollar business email compromise schemes ("BEC"). Although these pervasive schemes can take many forms, in a BEC, a hacker generally compromises a company's email server and performs some level of reconnaissance to identify the email account of a company employee/executive with access to, or authority for, company finances. Once identified, the hacker will use the compromised email account to impersonate the account owner to redirect authentic wire transfers to bank accounts controlled by the criminal enterprise, or to request the company to provide, and send to the criminal enterprise, authentic bank checks.

Although money is usually the principal target of these criminal enterprises targeting businesses, BECs also regularly target tax records of individual company employees to commit additional fraud. Businesses that regularly perform wire transfer payments and communications with foreign suppliers or businesses have been particularly vulnerable to BECs.

In illustrating the continued prevalence of this cyber threat, the Internet Crime Complaint Center ("IC3") indicates that in 2017, reported BECs alone caused losses of $676 million to companies and individuals, a figure that comprised nearly half of all reported losses due to cybercrime. Moreover, IC3 indicates that BECs have caused $3.7 billion in losses since IC3 began keeping statistics on these schemes.

A company's best defense against BECs is to proactively maintain adequate cybersecurity and data privacy measures. As part of these measures, employees should be trained on BEC risk in particular, as well as on how to identify suspicious emails to prevent unwitting compromise of company email accounts and networks. If a compromise occurs and a criminal enterprise is successful in diverting a wire or check to an unauthorized account or recipient, companies should be prepared to quickly coordinate with their banks and law enforcement to attempt to stop the transaction or recover sent funds.


James T. Kitchen
Pittsburgh


Mauricio F. Paez
New York


Lisa M. Ropple
Boston


Aaron D. Charfoos
Chicago
