FBI Issues Public Service Announcement About Recent E-Mail Scam Targeting Businesses

On June 14, 2016, the Federal Bureau of Investigation (FBI) issued a public service announcement relating to a recent surge in 'business e-mail compromise' (BEC) scams, which are sophisticated scams that target businesses through e-mail or other means in an attempt to induce a wire transfer to a fraudulent account. The FBI reports that between October 2013 and May 2016, U.S-based businesses alone have lost $960,708,616 as a result of BEC scams. Against the backdrop of these massive losses over the last three years, the FBI further states there has been a 1,300% increase in the amount of losses caused by these scams since January 2015 alone.

The FBI's Internet Crime Complaint Center (IC3) has identified five basic scenarios of BEC, all of which businesses should be on the lookout for. They are:

- **DataTheft**: Hackers gain control of the e-mail account of a key company executive. Using their access to that account, they e-mail an employee that is responsible for managing employees' confidential information, such as someone responsible for preparing tax forms, to request copies of such forms (i.e. W-2's) or other private information. That information will then be used to gain access to employee accounts, or to further some other sort of fraud.

- **Fraudulent Supplier Requests**: This method is often used to target businesses that have long-standing relationships with suppliers – which, of course, includes most businesses. A hacker gains access to the account of someone at the supplier (or sends an e-mail from an account with a very similar e-mail address) attaching a fraudulent invoice or wire transfer request.

- **Fraudulent Transfer Requests from Executive Accounts**: Hackers gain access to the e-mail account of key company executives, and e-mail others at the company requesting that a wire transfer be made promptly and discreetly in order to help the executive facilitate some sort of transaction.

- **Fraudulent Requests to Business Contacts**: Hackers gain access to the personal e-mail account of an employee and send requests for wire invoice payments or wire transfers to that employee's business contacts.

- **Executive or Attorney Impersonation**: Hackers contact an employee by e-mail or phone, and fraudulently identify themselves as a key executive or attorney for the company that claims to be working on a time-sensitive and confidential matter. The hacker then requests that a wire transfer be made promptly and discreetly in order to help with that matter.

Although it is nearly impossible to totally guard against and prevent such scams, the IC3 has identified best practices that it recommends businesses put into place immediately, if they have not done so already. For example, it is strongly recommended that businesses:

- Avoid the use of web-based or personal e-mail accounts for business matters;

- Avoid posting details about operations or hierarchy on social media or the business website;

- Beware sudden changes in business practices or unusual requests that appear to come from a supplier/vendor;
- Be suspicious of requests to act quickly or discreetly;
- When responding to e-mails, use the 'forward' button and enter or select the correct e-mail address for the intended recipient instead of relying on the 'reply' button;
- Consider implementation of a two-step verification process for significant transactions (i.e. require a supplier to verify a request for payment sent by e-mail) and/or two-step authentication (i.e. a password to log on, and another pin/key code to verify an employee's identity before log-in is completed);
- Consider purchasing and securing domain names similar to the one used by the company;
- Utilize verifiable digital signatures; and
- Create intrusion detection system rules for company e-mail systems that will flag/block e-mails with extensions that are similar, but not identical to, those used by the company.

The full public service announcement can be accessed at: http://www.ic3.gov/media/2016/160614.aspx. For more information, please contact Michael D. Billok, Clifford G. Tsan, Christopher J. Stevens, or the attorney in the firm with whom you are regularly in contact.

BOND SCHOENECK & KING ATTORNEYS

Commitment · Service · Value · Our Bond