Client Advisory

2 May 2018

Butterfield

Business E-mail Compromise Fraud

In recent months, there has been an increase in the incidence of Bermuda-based companies being targeted with a sophisticated, cyber-enabled fraud technique known as Business E-mail Compromise ("BEC"), also known as "CEO fraud". Law firms, trust companies, management companies and other professional services firms that execute payments on behalf of clients are particularly being targeted.

BEC fraud generally involves: (1) infiltration of a company's e-mail system through hacking, spear-phishing attacks or malware; (2) subsequent monitoring of the company's e-mails by criminals to determine the identities of requestors and authorisers of payments, and those who execute payment requests from company accounts; (3) sending fraudulent e-mails to employees who execute payments that appear to be legitimate requests for transfers/payments from company executives or clients who would typically request and/or authorise payments; and (4) the execution of a transfer or payment request by the targeted employee to the account(s) specified in the fraudulent e-mail.

Financial institutions are challenged to combat this type of fraud directly, as payments and transfer requests are received in the form of valid instructions from authorised individuals, and call-back verifications are typically authenticated by those same individuals who believe they are acting on legitimate client/executive requests.

Protecting Yourself From BEC Fraud

The most effective way to avoid becoming a victim of BEC fraud is to put in place internal protocols for the verification of payment requests that involve verbal approvals. In other words, when an employee receives a request for a payment by e-mail, he or she should verify its legitimacy in person or by telephone (using phone numbers on file, not those provided in the e-mail) with the purported requestor before executing the transaction.

Other safeguards include:

- Monitoring transactions closely and reconciling your accounts frequently, and immediately reporting any discrepancies or unauthorised activity to the Bank
- Setting up internal e-mail systems to identify external e-mails, or e-mails where the "reply" address is different than the "from" address
- Verify changes in vendor payment details by adding two-factor authentication, such as having secondary sign-off by company personnel
- The use and maintenance of network firewalls and anti-virus software

If you suspect you have been a victim of fraud, report it to us immediately by calling (441) 295 1111.