BUSINESS EMAIL COMPROMISE:

THE GLOBAL FINANCIAL THREA T

Business Email Compromise (BEC) is a strategically planned social engineering attack against businesses of all types and sizes. This scheme exploits vulnerable internal controls around monetary transfers and has caused devastating financial losses and the theft of confidential employee and/or company data.

KNOW THE HALLMARKS

Impersonation: Email requests for wire/ACH transfers appear to be from company executives or vendors and are typically sent to accounts payable and HR personnel.

Any type of business is vulnerable, including real estate or law firms, or companies where consumers are engaging in business activity.

Attacks have evolved to a more targeted approach using spear **phishing emails and phone calls** to collect information for use in an attack.

The impersonators will generally **convey a sense of urgency** and/or confidentiality related to the transfer of funds.

THE IMPACT CAN BE COSTLY

Financial losses increased over

2,300%

between January 2015 and December 2016.

More than

$5 BILLION

IN TOTAL LOSSES

between October 2013 and December 2016.

WHAT TO DO

IF YOU SUSPECT A **BEC** ATTACK YOU SHOULD:

- Immediately **contact your financial institution** and request a recall of funds due to fraud.
- Report it to your local **FBI office:** https://www.fbi.gov/contact-us/field-offices
- File a **complaint** with www.ic3.gov

Sources/Resources:
FBI – https://www.ic3.gov/media/2017/170504.aspx
Small Business Fraud Center – https://www.bankofthewest.com/security-center-small-business/fraud-center.html
Commercial Fraud Center - https://www.bankofthewest.com/security-center-commercial/fraud-center.html

BANK OF THE WEST
BNP PARIBAS

Member FDIC. Equal Housing Lender.
© 2017 Bank of the West.