A D V I S O R Y

FinCEN (Financial Crimes Enforcement Network), a division of the United States Department of the Treasury, is reporting e-mail schemes aimed at defrauding financial institutions and their customers.

KCB Bank wants to share this information with our valued customers to help you guard against these growing e-mail fraud schemes.

Email Compromise Fraud occurs when criminals compromise the e-mail accounts of victims to send fraudulent wire transfer instructions to financial institutions in order to misappropriate funds. These criminals target business e-mail accounts as well as consumer e-mail accounts. These schemes are among a growing trend of cyber-enabled crime.

Criminals unlawfully access a victim's e-mail account through social engineering or computer intrusion techniques. Then they exploit the victim's e-mail account to obtain information on the victim's financial institutions, account details, contacts, and related information.

Criminals use the victim's stolen information to e-mail fraudulent wire transfer instructions to the financial institution, appearing to be from the victim. Criminals have either taken over control of the victim's e-mail account or have created a fake e-mail account which closely resembles the victim's e-mail. The criminal tricks the employee or financial institution into conducting wire transfers that appear legitimate, but are indeed unauthorized. Below are example scenarios of how these schemes are executed.

E-Mail Compromise Schemes:

1. Criminals unlawfully access the e-mail account of a Company employee to send fraudulent wire transfer instructions to the Company's financial institution.

2. Criminals unlawfully access the e-mail accounts of a Company's executives or employees and impersonate them to directly submit fraudulent transaction instructions to the company's financial institution.

3. Criminals unlawfully access the e-mail accounts of a Company's suppliers to e-mail and inform the Company that future invoice payments should be sent to a new account number and location.

KCB Bank wants to share some best practices for keeping your email secure:

-Implement Spam Filtering on inbound email to block unsolicited email that may contain malicious URLs. Spam Filtering should validate that the email is coming from a valid email address and a valid domain before delivering the email to your inbox. Email authentication technologies, such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC), should be implemented.

Never respond to emails asking for personal information or login credentials.

Fraudulent emails can be hard to identify, but beware of emails that:

-Request you click on a link. This could be a phishing email that is impersonating a real company or organization and trying to get you to a spoof website. Since a fraudulent email may use exact wording from the real company's website, it can be difficult to identify. By clicking on an embedded link in a fraudulent email, you may inadvertently download tracking software or viruses that track your keystrokes to gain your personal information.

-Ask you to enter, confirm, or update sensitive personal information.

-Indicate a sense of urgency and asking you to provide information immediately to avoid a specific event from happening if you do not respond.

-Contain bad grammar or spelling errors. Intentional spelling errors may allow the email to bypass spam filters used by Internet Service Providers (ISPs).

-Utilize pop-up windows for entering or confirming personal information.

If you receive one of these types of emails, **do not** open any attachments or click on any links in the email. Delete the email and then delete again from your Deleted Items. Also make sure you delete Junk Mail on a daily basis.

Success in detecting and stopping these types of schemes requires careful review and verification of instructions. KCB Bank requires each transfer request shall be made by written request using facsimile, secure Bank Mail through Internet Banking, or presented in person to Bank personnel. KCB Bank employs a multi-faceted transaction verification process to verify the validity of a request. If the request is not performed in person, we will conduct a call back verification. We also consider additional indicators and the surrounding facts and circumstances, such as a customer's historical financial activity. Where appropriate, we conduct additional inquiries and investigations.

It is vital that we work together to detect and prevent fraudulent wire transfer requests. Please refer to our online resources, **KCB Bank Best Practices for Business Banking** and **KCB Bank Best Practices: General Internet Security**, located in the **ONLINE SECURITY INFORMATION** tab on our Homepage at **www.kcbbank.com.**