Bank of American Fork

February 1, 2017

FRAUDULENT EMAIL PAYMENT REQUESTS

Dear Business Customer,

Cyber criminals can use compromised email accounts to defraud your business. This letter is to inform you of a scam that has been attempted on some of our business customers.

Using compromised business email accounts, criminals attempt to identify customer, vendor, and employee email information from the email history. Criminals then impersonate the owner of the compromised email account and attempt to exploit and defraud the email contacts by sending emails containing fraudulent invoices or payment instructions. In many cases, the criminals are requesting that the recipients send payments via wire transfer.

To prevent financial loss, we recommend that you review your current internal business practices and strengthen any weaknesses you find. The risk of financial loss can be reduced by using verification and payment controls. We recommend that you:

- Have at least two individuals review payments before they are sent;
- Not process payments based on email requests without additional verification;
- Use telephone call-back procedures or other non-email-based means to verify payment instructions;
- Verify changes in vendor payment locations or requests;
- Train your employees to be alert and cautious with any email that requests a payment or sensitive information; and
- Strictly comply with all security procedures in our written agreements.

Strong payment verification controls could save your business from sending unauthorized payments, which often result in financial losses. If you have any questions regarding this letter, please contact a member of our Customer Service or Treasury Management teams at 800-815-2265.

Sincerely,

Joshua Everton
VP/eBanking Manager