Business Customer Email Compromise ("BEC") Fraud Scam
What You Need to Know!

WHAT IS A BEC?

You don't have to work in big organization to be impacted by business email scams - A BEC scam can trick both unsuspecting employees and company executives. Fraudsters use a hacked or fake email account that looks legitimate to trick the unsuspecting victim into sending money.

Criminals do not discriminate, with targets ranging from individuals and families to employees at various businesses including non-profit organizations. Some examples of what fraudsters do include (but are not limited to):

- Fraudsters attempt to take control of or otherwise impersonate (e.g., spoof) legitimate business customer email accounts (typically email accounts belonging to company executives or high-level employees)
- Fraudsters can also pose via email or text as someone the business customer trusts (typically a colleague, boss, or vendor)
- When the fraudster communicates with the business customers or their financial institution, they usually write in the email subject line that the transaction, transfer, etc. request is "urgent" or "time sensitive", or they use other language to indicate the matter is of utmost importance

EXAMPLES OF A BEC

- **Business Employee Impersonation Fraud** – Fraudsters pose as an employee of the business and typically email another employee within the finance department requesting funds be transferred to an account controlled by the Fraudster
- **Email Account Compromise** – A business employee's email account is compromised and used to request that a fraudulent transaction be made by a third-party (e.g., a vendor known to the business) or the business' financial institution
- **Attorney Impersonation** – Fraudsters impersonate a lawyer or legal representative to convince the business employee to facilitate a transaction or transfer to an account controlled by the Fraudster

HOW TO PROTECT YOURSELF

Be alert, business email scams can appear to come from legitimate sources, including:

- **A vendor** – The email arrives from a hacked or spoofed email address to notify you of a bank account change or to request payment
- **A familiar email address** – The email appears to come from someone you know instructing you to process a payment or to provide confidential information

Be Prepared	If You Think You Are a Victim
• Verify payment requests in person or by calling the vendor/individual at a known number to make sure it is legitimate. Avoid confirming by email or text. • Confirm any change in the account number or payment details • Ensure that the individual confirming the details is familiar to you or can be verified as having authority to confirm the changes • Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight variations to trick your eye and gain your trust. • Ensure your staff are trained on how to identify and report potential phishing attempts	• If you believe you have been a victim of fraud, please contact your Banking Team, reach out to Valley's Customer Care Team at 800-522-4100, or connect with us at valley.com/security. • Report the fraudulent activity to law enforcement and file a complaint with the FBI's Internet Crime Complaint Center (IC3) • Document everything about the event. The more information you have, the better prepared you will be to assist an investigation.