Using Cash Management Securely

Corporate Account Take Over is a form of business identity theft in which criminals steal a business' online banking credentials and then use those credentials, without authority, to initiate fraudulent online banking activities. Criminals will often research their victims using business networking sites or social media. Then they send emails to you or your employees with attachments or links that contain malicious code. Once those attachments are opened or the links are clicked, malware spreads onto your computers, gathers information about your online banking activities, and sends that information back to the criminal; all without your knowledge.

You and your employees are the first line of defense against corporate account take over. The safe practices described below, combined with employee education about the warning signs and prompt responses to suspected take over, are vital to protecting your business, your customers, and your bank accounts.

- Use a restricted workstation for your Cash Management online banking activities and do not allow web browsing, email, clicking links, or opening of unexpected attachments at that workstation;

- Provide continuous communication and education to employees who have access to your online banking systems about the "Never Rules at Work". Never click links in an email, never open unexpected attachments, never download free music or games, never participate in file sharing sites, never open e-greeting cards, never use free scanning software, never disable anti-virus controls, and never give out business information on unsolicited sales calls;

- Utilize all bank controls including enrolling your Cash Management computer in Trusteer Rapport offered free from Pentucket Bank. This security solution is designed to safeguard you and your bank accounts from online threats;

- Continually maintain up-to-date anti-virus and regularly install security patches;

- Adhere to dual control procedures: one authorized employee completes ACH batches and wire transactions and, from a separate computer, a second authorized employee approves and submits the batches and wires;

- Practice daily account reconciliation, especially near the end of the day;

- Adopt advanced security measures by working with consultants or dedicated IT staff set passwords on your wireless access and maintain a fire wall.

- Contact Pentucket Bank immediately if you suspect fraudulent transactions, if the Cash Management online banking pages appear different or you receive an email claiming to be from the Bank requesting information.