To: **Our Community Bank Customers**

From: **Bankers' Bank of the West Executive Team**

Date: **August 20, 2013**

By now you've probably heard that a crime commonly known as corporate account takeover was committed at banks in the mountain states and Great Plains region earlier this summer.

The fact is, **any** bank—of any size, in any region—can fall prey to cyber criminals.

The intended victim

The main target of a corporate account takeover is a financial institution's business customer, not the bank itself. The crook sees the corporate customer as more vulnerable than the (presumably) well-secured financial institution. Using a mix of techniques—generally involving spyware that monitors corporate employees' keystrokes to steal passwords and other sensitive information—the criminals might take several months to plan their attack. Then they attempt, and often successfully pull off, a quick online heist of hundreds of thousands of dollars. Because many such thefts are perpetrated from far-off corners of the world, most of the crooks are never caught.

Keep in mind that **either the corporate customer or its bank, or both, frequently suffer huge losses** when a corporate account takeover is committed. This underscores the need for the corporate customer as well as the bank to maintain high security standards; otherwise, both could become susceptible to attack. To borrow a proverb, a chain is only as strong as its weakest link.

Build a tough defense

The value of staying current on developments affecting banks, especially in the area of cyber security, cannot be overstated. Scam artists regularly adapt their tactics to changing conditions, after all. Don't allow yourself to become complacent.

Following are some commonsense steps to help you control risk to your bank and your corporate customers:

1. **Educate your customers**—especially businesses. Update them on the tactics being used by criminals. Let them know the biggest security risks are human-related. For instance, scammers are constantly tweaking their social engineering tactics (like phishing) in an effort to trick victims into downloading malicious software. Also stress the need to secure any "bring your own" smart devices used by employees in the workplace—including tablets, smart phones, laptops, and e-book readers.

FOR BANKS USING BIDS

While automated risk management tools are no substitute for following proper risk management rules and procedures, they can significantly reduce the potential for inconsistency and human error. What's more, they can help ensure regulatory compliance.

The ACH Risk Management solution available through BIDS is equipped with a full complement of helpful features including real-time notification of limit exceptions.

For more information on BIDS' competitively priced ACH risk management solution, contact us at **800-873-4722** or bbwadjustments@bbwest.com.

2. Make employee vigilance a high priority **at all levels of your bank**. In addition to knowing the customer, you need to know your customer's routine banking behavior. Watch for changes in established patterns. Question anomalies. If out-of-the-ordinary activity occurs on a commercial account, shut down access immediately.

3. Engage your customers in **fraud-prevention efforts**. Some banks provide anti-malware software, and regular updates, to customers with online access. If such an expense is out of the question, consider at least providing best-practices guidance and software recommendations for business customers.

4. Make certain that verifiers at your bank **critically review all ACH files before** sending them through. This step is a linchpin in your security scheme.

5. Require business customers to follow **dual control** when originating ACH files. Never release an ACH file before getting a receipt from a second authorized individual at that business.

6. Specify in your agreements that customers must maintain balances sufficient to cover any unfunded files—both debits and credits.

7. Warn your business customers against originating ACH files from any computer that isn't properly secured—for instance, a laptop on a public network. Consider including language in your agreements that expressly prohibits the customer from originating ACH files from a non-secured computer. Or advise customers to use a dedicated computer for online access.

8. Keep a current *ACH Risk Management Handbook* (a NACHA publication) nearby. You can order a copy from NACHA or get one through your regional payments association.

9. Earmark both funds and staff time for the ongoing education and training of bank employees. Even a modest commitment represents a wise investment in these changing times. Urge key employees to become certified in areas of expertise most crucial to their function. Enroll appropriate staff in courses, webinars and conferences offered by your state banking associations, your payments associations, and other professional groups. Invite employees to share security-related information with their co-workers.

Another abundant source of resources is the Internet. Among the many worthwhile websites are the Financial Crimes Enforcement Network website; the members-only section of American Bankers Association website; and Risk Radar, a Federal Reserve Bank services resource.