

The ABC's of keeping your account information secure

- **ACH Limits**- Set appropriate ACH exposure limits that are very close to daily activity. In most cases, a fraudster won't know a company's daily limit and may exceed it when sending a fraudulent file; this activity will alert require manual intervention and facilitate a call to the legitimate customer.
- **"Business use only"**- Designate one workstation that is used only for online banking and payments. This will help to prevent the inadvertent downloading of malware or other viruses by users visiting websites and clicking links in an email.
- **Check your accounts frequently**- Reconcile corporate bank accounts daily if possible. Many corporate clients, particularly small business clients, may not typically reconcile their bank account on a daily basis, and therefore may not recognize fraudulent activity until it is too late to take action.
- **Dual control**- One of the most effective controls is for corporate customers to always initiate ACH and wire transfer payments under dual control. For example, one individual initiates the creation of the payment file, and another approves the file for release.
- **Ensure that the computer's operating system and its components are up-to-date with current software patches.** For example, the use of the most current firewalls, malicious code filtering, virus protection and spyware removal software will aid in the control of network intrusion tactics.