Minimizing your exposure to fraudulent activity

Access US – September 2016

With fraudulent activity on the rise, it's important to establish internal procedures to guard against fraud and abuse. This article outlines some of the actions you can take to help your company reduce the risks associated with fraud.

Card payment best practices

- Ensure that your POS (point of sale) system is EMV (Europay, MasterCard® and Visa®) compliant. EMV technology adds an extra layer of security to help protect you and your customers from fraud. The chip virtually eliminates counterfeiting, and is now the security standard across Europe and beyond.

Electronic payment best practices

- Review ACH (automatic clearing house) and wire-transfer procedures on a regular basis and make sure that user credentials are updated and maintained to meet appropriate needs.
- Use ACH Positive Pay to monitor and control ACH transactions before they post to the bank account and allow transaction acceptance or rejection in real time.

Check payment best practices

- Reconcile accounts on a daily basis.
- Migrate from check payments to electronic payments.

Online best practices

- For the highest level of security, conduct all online banking activities from a stand-alone, hardened and completely locked-down computer system from which email and web browsing are not possible.
- Turn on automatic notifications to alert you of transaction status changes

System best practices

- Review users' needs for administrative rights. If possible, limit administrative rights on computers to help prevent the inadvertent downloading of malware or other viruses.

For additional fraud prevention suggestions, visit the Bank of America Small Business Community at bankofamerica.com/sbc or contact: Ted Janicki, Vice President, Tel: 716.394.7747, Email: thaddeus.m.janicki@baml.com