Signature Bank

The dos and don'ts of fraud protection

Fraud is often top of mind for consumers, but many companies overlook the threat fraud poses to their business until it happens to them.

Recently, one of our customers was a victim of fraud. A fraudster installed malware on an executive's computer enabling access to the customer's on-line banking accounts. When the customer logged in, the fraudster "piggybacked" on his session. Once inside, the fraudster created a wire and ACH transaction, but couldn't get past the security questions. Fortunately, the transactions were stopped before any money was lost.

The threat of fraud is ever-present and growing as fraudsters become more sophisticated, creative and aggressive. No fraud prevention approach is infallible, but to protect your company against fraud, you and your bank should have rigorous programs in place.

Six DOs and DON'Ts of fraud protection

DO	DON'T
DO work with an IT professional to install antivirus and antispyware programs.	**DON'T** let software updates lapse. Many companies think they are covered once they put the software in place, but become vulnerable when they don't stay on top of program upgrades.
DO proactively establish anti-fraud employee policies regarding e-mail, instant messaging, social media, pop-up ads and downloading software.	**DON'T** forget frequent employee communications about these policies and the potential consequences when they are not followed.
DO use firewalls at all times.	**DON'T** ever turn your firewall off, even a minute can leave you vulnerable.
DO take advantage of the latest anti-fraud measures like positive pay and internal dual control catch check and ACH fraud before fraudulent transactions go through.	**DON'T** assume anti-fraud software is enough – you need multiple barriers to effectively protect yourself.
DO work with your bank to understand their fraud protection program.	**DON'T** rely solely on your bank's efforts to protect your company from fraud. To be effective, measures need to be taken by both your bank and your company.
DO be vigilant. Keep a close eye on your accounts and alert your bank immediately of any suspicious activity.	**DON'T** underestimate the potential damage fraud can cause to your company.

Signature Bank's Fraud Program

Signature Bank has a multi-tiered approach to protect our customers from fraud. This is important because if one barrier fails, there is another in place to prevent money loss. Our platform includes:

- Best practices for token authentication, security questions, watermark verification and dual approval policies.
- Analytical software identifies behavioral anomalies and alerts us when something is suspect or out of the ordinary.
- Bank employees who monitor our customers' activity, daily. These watchdogs' familiarity with our customers and their behavior provides an extra layer of protection.

Did you know?

Fraudsters strike when you are least likely to notice. During holiday and summer months, people are busy—personally and professionally—and may not be monitoring their accounts, that's when fraudsters take advantage. They also tend to strike later in the week. They know people often aren't checking their accounts over the weekend. Constant monitoring and vigilance is critical to protect your company.

Anne C. Doligale
Senior Vice President
Treasury Management Consultant
(312) 506 3413
adoligale@signature-bank.com
www.signature-bank.com