FARM CREDIT

FRAUD PROTECTION AWARENESS SERIES

Fraud Tip #8 – Fraud Prevention and Best Practices

Fraud scams affecting U.S. businesses show no signs of going away. According to the FBI's Internet Crime Compliant Center (IC3), schemes compromising business and personal email accounts were responsible for more than $360 million in business losses in 2016. More than 12,000 U.S. businesses fell victim to these schemes, accounting for the highest losses among all cybercrimes tracked by IC3.

Fraud loss recovery efforts can be complicated. Early detection and prompt reporting of fraud is critical because the passage of time might adversely affect the potential for recovery or the outcome of a customer claim. Your attentiveness often is the first line of defense. If fraud occurs, your diligence may be what makes the difference between recovery and loss.

To help your business avoid these and other fraud schemes, we are beginning our 2018 Fraud Awareness series with a discussion of best practices for identifying and preventing potential business fraud. We urge you to incorporate these practices into your operating procedures.

Daily Reconciliation – Identify & Report Fraud Immediately

Prevention is key, but it is critically important to identify – as soon as possible – any fraud that may have occurred by monitoring and reconciling your account activity every single day. Comparing your records against bank records online will allow you to identify any unauthorized or unusual payments and take immediate action.

If you identify fraud or unauthorized transactions on any of your accounts, contact your bank immediately. Commercial fraud should also be reported to your local law enforcement agency and/or the FBI. Information about when and how to contact the FBI is available at https://www.fbi.gov/contact-us/.

Build Employee Awareness

It's hard to overstate the importance of employee awareness in preventing fraud. Today's fraud schemes are so sophisticated that there are many potential points of entry into an organization. One of the most effective ways for a business to avoid becoming a fraud victim is through ongoing employee awareness:

- If you don't already have a fraud training program in place, a great way to start is by distributing these fraud tips to your employees.

- The Association of Certified Fraud Examiners is another great resource for fraud training materials. Videos, infographics and other information are available at http://www.fraudweek.com/resources.aspx.

Confirm Vendor Account Changes and Payment Requests through Alternate Channels

A best practice for avoiding vendor fraud schemes is to confirm any request for changes to a vendor's payment information – name, address, bank account – by calling a known vendor representative. Also:

- High-dollar vendor invoices received by email should be authenticated by phone with the vendor prior to payment.
- For invoices received by U.S. mail or overnight delivery service, phone or email is appropriate.
- Communicate with vendors using only the vendor's established phone number, email address and contact names on file. Do NOT call or email using any information on the received invoice.

Secure Blank Check Stock and Mail Checks in a Secure Location

Much of the fraud committed against businesses has moved online, but unfortunately, check fraud continues to increase and thrive. Some best practices for eliminating check fraud:

- Store blank check stock and/or cancelled checks in a secure location and limit access only to specific employees authorized to handle check payments.
- Outgoing check payments should be mailed from a secure/locked location and not placed in an open outgoing mail area. Intercepted checks often get stolen from unsecured mailboxes, both outgoing and incoming.

Keep in mind, fraud protection regulations for commercial accounts differ significantly from consumer accounts. A business only has until the next business day to reject an unauthorized check posted to its account to ensure the funds are recovered. Due to this very short return window, Positive Pay services are the ONLY effective protection against check fraud losses.

Use Check and ACH Debit Positive Pay to Monitor Payments

Positive Pay services are designed to help protect against the payment of altered and counterfeit checks, as well as unauthorized ACH payments. Positive Pay has several variations:

- In the basic version, a customer uploads an electronic file with issued check information to the bank each day. As checks clear, the bank matches them to issued check records by date, check number and amount. Any discrepancies are flagged for review.

- There is also an option to match check payee names. Any mismatches are identified as exceptions for the customer to review and approve online before the daily deadline.
- Reverse Positive Pay is an alternative for customers not able to upload issued check files. This service provides the customer with online images of all checks clearing each day. The customer reviews the images and indicates the decision to pay or return each item.
- ACH Positive Pay permits customers to view and filter ACH debit entries and decide to pay or return all exceptions. Any ACH debit entries that do not have a pre-approved ACH Payment Rule in place for auto-acceptance will be flagged as exceptions for review and decisioning.

Strengthen Internal Controls - Separation of Duties / Two-Touch Approval Process

Strong internal controls are a critical component in preventing fraud. Best practices include:

- Separating duties in the accounts payable and payments disbursement processes. More than one employee should be involved in the processes of approving payments, generating checks or ACH payments, signing/approving checks and sending payments. Separation of these duties provides multiple checkpoints for identifying unauthorized payments.
- Implement a two-touch process for approving payments. Each approver should have a strong knowledge of the accounts payable process and the company's vendor/payments universe. Their knowledge should include what constitutes typical vendor or outgoing payments behavior in order to identify – and escalate – any anomalies.
- Require verbal (phone or in person) confirmation of any internal request for an outgoing payment to a new recipient/vendor, or to a new bank account number of an existing recipient/vendor. Business email compromise is one of the most successful fraud techniques in use today, resulting in billions of dollars lost. Individuals' personal email accounts can be easily hacked or spoofed, and the fraudster is relying on your employee's presumption that an emailed request from a company leader will not be questioned or verified. It's critical that this confirmation be verbal – not by email – because you may in fact be communicating with the fraudster.