BUILT FOR
BETTER BUSINESS

Keeping your information safe

WIRE FRAUD & SMALL BUSINESS

As a small business, fraud prevention is likely a significant area of concern. While there are several tasks to accomplish each day for successful business operations, preventing fraud can be one strategy to help protect your bottom line. Each year, fraud takes a toll on companies large and small, but in recent years, criminals are increasingly targeting local small businesses. The key trends along with action items for business owners to follow in an effort to prevent fraud are identified below. No matter how prevalent you think fraud is among small businesses, this information offers an opportunity to put in place the safeguards necessary to protect you and your customers.

Fraud Trends

The 2018 Association for Financial Professional's Payments Fraud Survey found that payments fraud reached a new high in 2017. A record 78% of all organizations were hit by payments fraud last year, according to the survey of nearly 700 treasury and finance professionals. Checks continue to be the subject of more deception than any other payment method, with 74% of respondents reporting this form of attack. However, wire fraud followed at 48%, while corporate card fraud ranked third at 30%.

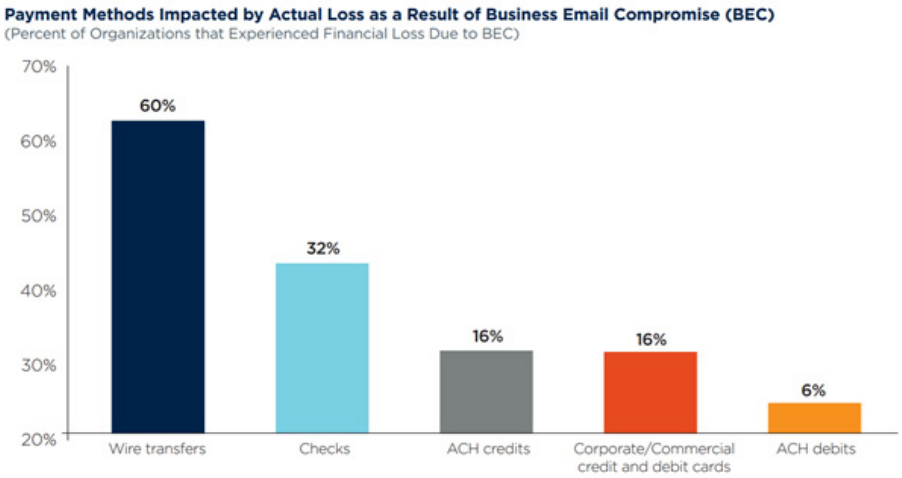
Wire fraud scams often victimize two businesses – the company expecting to receive payment, and the organization that thought payment had been made. The crime of wire fraud can cause significant contractual disputes between the victims as to who should bear the loss. The following is a snapshot of information concerning wire transfer fraud.

Source: 2018 AFP Payments Fraud and Control Survey

Common Wire Scams

Consumers and businesses are periodically conned into wiring money to nefarious actors most often via licensed money transmitters like Western Union and MoneyGram. Once a consumer sends money to a scammer, it is often impossible to find the fraudster or retrieve the money. What complicates matters is the reality that wire fraud criminals are located both inside and outside of the United States. As a business owner, it is necessary to recognize the most common wire fraud scams which include:

- **Business Email Compromise/Email Account Compromise:**
  Imagine a typical day at the office. An employee receives a friendly reminder email from a vendor they've known for years about an invoice coming due. The email is conversational, asks about the employee's recent vacation, and then reminds the employee that a late payment for the invoice could result in a surcharge if not handled immediately. Communications like these may be the work of a wire fraud criminal.



Source: 2017 AFP Payments Fraud and Control Survey

- **Utilities:**
  A scammer tells the consumer that their utility (power, water, cable, etc.) will be shut off if they do not send money or gift cards immediately.
- **Relative in Need:**
  A fraudster poses as a consumer's family member, often a grandchild or a distant relative, and claims that they need money for an emergency.
- **Lottery or Prize:**
  A scammer tells the consumer that they won a lottery or prize money but they must send money to claim it.
- **Debt Collection:**
  Posing as a debt collector, a wire fraud criminal uses threats to make the consumer settle a fake debt.
- **Purchases, Sales, and Leases:**
  A fraudster tells a consumer that money must be sent to complete a purchase, sale or lease.
- **Employment Offers:**
  A scammer poses as an employer, gives a consumer a fake offer of employment, and tells them to send money in connection with the offer of employment.
- **Online Dating**
  A scammer poses as an online dater, contacts a consumer who is dating online, and asks for money as a gift or to help with an emergency.
- **Secret Shopper:**
  A wire fraud criminal sends a consumer a check with a letter instructing them to deposit the funds. The scammer then tells the consumer to go to various stores and purchase items, to wire money to the scammer, and not to tell the money transmitter why they are wiring money.
- **Advance Fee Loans:**
  A scammer poses as an online lender and after the consumer submits a loan application, they are directed to wire processing payments to the lender. Once the consumer wires the money, the loan is never received.

Action Items for Small Businesses

Several strategies can be put in place to make it more difficult for criminals to commit wire fraud. Small businesses may consider the following action items:

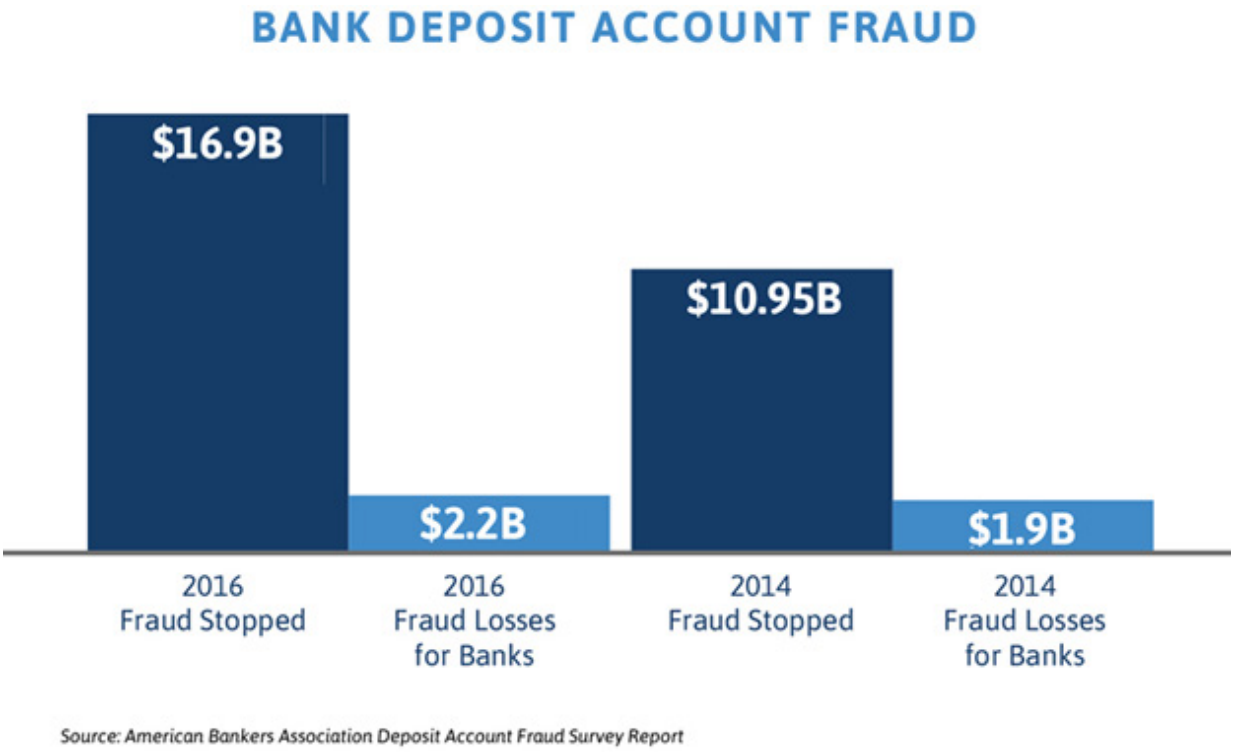
- ✓ Avoid free web-based email systems to transact business.
- ✓ Require employees to select unique and strong passwords or pass phrases.
- ✓ Require employees to change email passwords frequently.
- ✓ Require multi-factor authentication (e.g., email and telephone call) when receiving initial payment information or a request to change payment information.
- ✓ Send a confirmatory letter or email (not using the "reply" feature in email) concerning any request to change payment information.
- ✓ Delay payment in connection with any request to change payment accounts or a request to make payment to a foreign bank account.
- ✓ Provide clear instructions to business partners concerning how payment information should be communicated.
- ✓ Get all changes to vendor payment a ccount numbers in writing and verify with a phone call the number you have on file is correct. Keep account authorizations up to date and notify the bank when an authorized signer or online banking user leaves.
- ✓ Review any request received by email to change payment accounts for signs that the email may be from a third party.
- ✓ Tightly limit access on who can manage recipient information to prevent changes to key fields like beneficiary account information and monitor changes to these fields, paying close attention to payroll files.

- ✓ Run background checks and credit checks on all new employees who have access to your finances and continue to reinforce not sharing your online credentials via training.

If you are potentially impacted by wire fraud, you should:

1. Notify the receiving bank and request that a freeze be placed on remaining funds.
2. Notify law enforcement.
3. Investigate whether your email system may have been compromised.
4. Ask business partners to investigate whether their email systems may have been compromised.

Although wire fraud continues to be a concern for small and large businesses alike, the banking industry has taken proactive steps to help thwart scams that involve wire transfers. In 2017, banks have been able to prevent $9 out of every $10 of attempted deposit account fraud. However, small businesses need to be aware of the prevalence of wire fraud, and recognize that fraud prevention is an ongoing, critical business task. Combined with bank efforts, small businesses can take small steps to reduce payments fraud over time.



Source: American Bankers Association Deposit Account Fraud Survey Report

Top Resources

Use the following resources to learn more about payments fraud and its impact on small businesses.

American Bankers Association. Deposit Account Fraud Survey Report.*

Association for Financial Professionals. 2018 AFP Payments Fraud Survey.*

*You will be linking to another website not owned or operated by the bank. We are not responsible for the availability or content of this website and do not represent either the linked website or you, should you enter into a transaction. You are encouraged to review the privacy and security policies which may differ from ours.