Dollar Bank

Business Insights

Fraud Update:
How Scammers Are Targeting Businesses

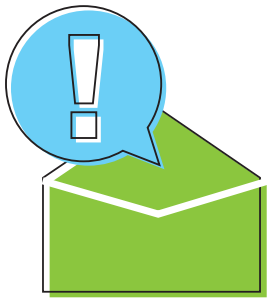
- **Business E-mail Compromise (BEC)**
- **Internal Fraud**
- **Data Breaches and Other Cyberattacks**

Business fraud, illegal activity that takes your company's money and puts it into someone else's pocket, is a growing threat. The Association of Certified Fraud Examiners estimates that organizations lose about five percent of their gross revenues to fraud.[1] Sometimes this fraud is committed by a random cyberthief; other times, by a customer, a vendor or even an employee.

Being aware of the types of fraud and how they are being perpetrated against companies can help you protect your own business. The following is information about some common types of fraud, along with precautions you can take to help keep your business safe.

Business E-mail Compromise (BEC)

The threat: BEC scams involve cybercriminals who compromise legitimate business e-mail accounts to conduct unauthorized transfers of funds. These typically involve "spoof" e-mails, which appear to the recipient to come from a known source while they are actually counterfeit messages from a perpetrator.



BEC losses topped $1.2 billion in 2018, nearly double that of 2017.

Source: FBI 2018 Internet Crime Report

For example:

- An e-mail that appears to be coming from an established vendor may announce a change in payment instructions. When the employee recipient makes this change, they unwittingly redirect funds to an illegitimate account.
- A business leader's e-mail may be spoofed so that it appears they are instructing an employee to initiate a wire transfer. The employee dutifully carries out the assignment only to discover later that those funds were directed to a fraudulent location.
- Employees may receive a "phishing" e-mail, luring them to click on a link to a bogus website where they are asked for IDs, passwords or other sensitive information that provides the scammer with access to payroll or other internal records that enable them to tap into funds. Alternately, an employee's click on a nefarious link or attachment may enable the download of malicious software (malware) such as ransomware, viruses and spyware, which can compromise sensitive data, offer the scammer the means to extort the business or take down the entire IT system.

The scope, sophistication and frequency of BEC schemes continue to grow, so it's important to stay alert and be able to recognize a scam in the making.

[1]Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse, Association of Certified Fraud Examiners

What you can do: Educate yourself and your employees about BEC and make a point of keeping up to date on the latest scams. Ongoing security education can help your employees recognize spoof e-mails and suspicious e-mail requests. Put processes into place for verifying wire and payment requests before they are carried out. Also ensure that your systems are adequately protected by a firewall and antivirus technology, that employees are using strong passwords and that your team updates software security patches as soon as they become available.

Internal Fraud

The threat: As much as you may not ever want to think your employees could be capable of committing crimes against your company, internal, or occupational fraud is a reality among businesses of all sizes. Companies with fewer than 100 employees are particularly vulnerable, says the Association of Certified Fraud Examiners, usually because business owners are unaware of this threat and because smaller companies may not have the resources to put adequate internal controls into place.

Occupational fraud may include any of a vast number of schemes. Asset misappropriation tops the list with activities such as cash theft, check tampering, payroll and billing schemes, etc. Employees may leverage their positions to build relationships with vendors or customers that put them closer to vulnerable information and processes, and when they collaborate with other employees, the potential for corporate losses grows. Data theft and bribery and corruption are common types of internal fraud as well.

What you can do: Hire thoughtfully, including conducting a thorough background check on every candidate. Never put an individual employee in charge of an end-to-end process involving finance, and trust but verify: Internal controls, such as data monitoring/analysis and surprise audits may help you detect irregular activity early on.

Median Loss per Employee Fraud Incident

Small businesses lose almost twice as much.

Fewer than 100 employees
$200,000

100+ employees
$104,000

Source: Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse, Association of Certified Fraud Examiners

It's also important to minimize temptations and add controls to protect your business accounts. For example, set spending limits on corporate credit cards and limit where they can be used. Monitor your bank accounts electronically for real-time transparency and take advantage of remote deposit capture, scanning and sending digital images to the bank rather than allowing paper checks to leave your office.

Most importantly, set the expectation of ethical behavior and nurture a culture of integrity.

Data Breaches and Other Cyberattacks

The threat: We hear a lot of news about cyberattacks (data breaches in particular) when huge corporations are involved, but cyberthieves attack businesses of all sizes. What's their intent? Stealing customer and other sensitive data, holding IT systems hostage until a specified payment is made (online extortion), infiltrating and damaging your computers and networks, etc.

What you can do: Ensure that your systems are adequately protected by a strong firewall and antivirus technology and update software security patches as soon as they become available. Software-at-rest protection is available, too, as encryption tools render any stolen data useless to the perpetrator. Consulting with a technology security expert about the potential need for vulnerability scanning, which will identify any weaknesses in your system, is prudent as well.