## Frauds Target Small Businesses: Don't Be a Victim

While large firms may have sophisticated technology and staff dedicated to thwarting crime, many small businesses don't — and scammers know this. Here are ways to protect yourself:

Be on guard against inside jobs. This includes employee theft or misuse of cash, merchandise or equipment as well as fraud. "Minimize risks through steps such as pre-employment background checks, automated inventory tracking systems, audits, and clearly outlined policies for personal use of computers and other business equipment," said Luke W. Reynolds, Chief of the FDIC's Outreach and Program Development Section. "Also, carefully select who handles revenue from customers, pays the bills and reviews account statements. And, ensure that there are procedures in place to detect and deter fraud."

Watch out for fraudulent transactions and bills. Scams can range from consumer payments with a worthless check or a fake credit or debit card to fraudulent returns of merchandise. Be sure you have insurance to protect against risks. Also ignore offers to buy lists of federal grant programs. To learn more about protecting your business, consult your local Small Business Administration District Office (www.sba.gov/content/find-local-sba-office).

Electronic frauds by third parties can be very costly to businesses, so take them seriously. The FDIC has seen an increase in reports of unauthorized electronic transfers made from bank accounts held by small businesses. "The most common and dangerous scam for small businesses is account takeover," said Michael Benardo, Chief of the FDIC's Cyber-Fraud and Financial Crimes Section. "By sending fake emails and using fake Web sites to deliver malicious software, such as keystroke loggers, fraudsters may be able to obtain the IDs and passwords for online bank accounts and then make withdrawals from accounts."

Because businesses are generally not covered by federal consumer protections against unauthorized electronic fund transfers, a bank likely will not be responsible for reimbursing losses associated with the theft from the account if it says that negligence on the part of the business, such as falling for a common scam, was a factor.

Also equip your computers with up-to-date anti-virus software and firewalls (to block unwanted access). Make backup copies of critical business data on every computer. Also monitor account balances regularly, perhaps daily, to look for suspicious or unauthorized activity.

And, don't click on links in or attachments to an unsolicited email that asks for confidential information, even if it appears to be from a company you do business with or the government. Legitimate organizations won't request that kind of information in an email. When in doubt, go to another source to find the organization's contact information so you can independently confirm the validity of the request.