

Businesses Beware of Mass Marketing Scam

August 18, 2009

Below is an alert that was just recently published by the FBI. This newest scam is targeting businesses and if unaware could end up costing your business hundred's if not thousand's of dollars.

There are steps your business can take to prevent these losses. The most important is educating your employees to common fraud schemes.

If you have any questions regarding scams directed towards individuals or businesses please speak with a bank representative.

Headline Archives

BUSINESSES BEWARE Of Mass Marketing Scams

08/14/09

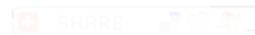


Almost everyone has heard horror stories about individuals who have been taken in by mass marketing fraud schemes—from phony sweepstakes to lottery scams. But here's something you may not know: the very same fraudsters who target individual consumers also target businesses.

Illicit mass marketers know that the keepers of corporate funds may be just as susceptible to fake ploys as anyone else. And while business-oriented fraud usually results in losses of a few

hundreds dollars the first time a company is hit, employees may continue to fall victim to these scams if the company has insufficient internal controls.

So what sort of mass marketing frauds are perpetrated against businesses? Here are just a few examples of what might happen to your companies:



- Masquerading as your usual office supplies provider, a fraudulent mass marketer contacts your employees, offering products at reduced or current prices in anticipation of impending rate increases. After paying the invoice, your company never receives the supplies it purchased.

- Your organization is asked to buy ad space in a business directory. The directory never sees the light of day, or only scammed companies like yours receive a copy.
- Criminals send invoices for unordered or undelivered products showing higher-than-agreed-upon prices, trying to exploit poor communication channels that may exist in your company and hoping that phony invoices will be paid without a second look.
- Your business receives an information packet offering to create and host your website. The packet includes a card that must be returned in order to "opt out" of the service, but the card is simply ignored or thrown out. Your company is then billed for web services it never ordered.
- In a variation of the [advance-fee scheme](#) that often targets individual consumers, perpetrators—usually targeting small businesses—offer low interest loans in exchange for an advance fee. You pay the fee, but your business never receives the loan.

While the FBI and other law enforcement agencies vigorously investigate frauds of all kinds, there are steps your businesses can take to protect themselves. For example:

- Educate yourself and your employees—especially frontline and accounts payable and receivable personnel—about common fraud schemes;
- Always ask for offers in writing, and require a written contract or purchase order for ANY transaction;
- Carefully review all invoices and compare them to expense records to make sure they are legitimate (and keep all records!);
- Use a credit card for purchasing supplies and services (if the vendor fails to deliver, you can dispute the charges);
- Don't give out full names of employees, as fraudsters can obtain an employee's name and then later claim this individual authorized the purchase of a product or service; and
- Be wary of accepting checks, because in some cases perpetrators have conducted a series of smaller, legitimate transactions to enhance their credibility and then used a counterfeit check to pay for a large order.

If you suspect you've been scammed, file a complaint with the Federal Trade Commission's [Consumer Sentinel](#), a database accessed by law enforcement agencies around the country. You can also contact [your local FBI office](#).

For more advice on how to protect yourself and your companies from fraud, visit our "[Be Crime Smart](#)" website.