OFFICE OF CONSUMER PROTECTION

Invoice Scams: A Warning to Businesses and Organizations

July 2016

A Warning About Phony Invoices

What businesses need to know

Invoice or bill scams are a **classic** form of fraud where a scammer sends out fake but real-looking bills or invoices in hopes that the victim will pay. Such scams usually target businesses and non-profit organizations. According to a United States Postal Service **report**, every year businesses pay out millions of dollars to phony invoice schemes. Scams may go on for months or even years before victims discover the problem. These invoices may arrive by mail or by email.

> *"every year businesses pay out millions of dollars to phony invoice schemes."*

The reason this scam works is simple: busy accounting departments or inefficient firms assume if they get a bill, they must have ordered the goods. Sometimes, the scammer will make sales calls to collect names of decision makers so they can then include that name on the invoice and make it appear legitimate. Others send unordered, low-quality office supplies together with an invoice for an inflated sum. Many times, the invoices are solicitations for *future* orders **disguised** as bills for *prior* orders. In fact, the **fine print at the bottom** may contain disclaimers in a bid to avoid criminal liability.

If you have been a victim of these scams, or if you have any questions about a merchant's activities, please contact the Office of Consumer Protection.

100 Maryland Avenue
Suite 330
Rockville, MD 20850
Main: 240.777.3636
Tip Line: 240.777.3681
Fax: 240.777.3768

You can also file a complaint online by clicking **HERE**

These invoice scams are often for office supplies, but according to the **Federal Trade Commission**, they can also be for social media features, directory listings, internet domain renewal, charitable contributions, solicitations disguised as refund or rebate checks, or magazine subscriptions. Some **enterprising scammers** will divert payments for legitimate invoices by contacting you claiming to be a representative of a current supplier and informing you that payments need to be directed to a new address or bank account--theirs.

How to Protect Your Organization

Do's and Don'ts

All is not lost. There are simple steps you can take to recognize scams and keep from being victimized.

- **Alert your staff.** An aware staff is a suspicious staff.
- **Have a specific individual do your supply ordering.** If there is only one person in charge of ordering, that person will know a suspicious shipment or invoice when it is received.
- **Keep that person's name private.** Do not let the receptionist or other staff members answering the phones to give out the name of the person in charge of ordering supplies when solicitors call.
- **Know who your supply representatives are what your contracts entail.** If someone calls saying they are your new account representative or that your supplier sold its business to another company, call that supplier back separately and verify.
- **Don't pay bills unless you can verify a 3-way match.** The invoice should match the shipping documents that arrive with the goods and the purchase order your business submitted.