

## Identity Thieves Target Businesses

Consumers are not the only ones to fall victim to identity theft. As Better Business Bureaus are discovering, small businesses are not immune to identity theft scams.

- The BBB in Winnipeg, Manitoba warns about local businesses that are receiving faxes purporting to be from the U.S. Internal Revenue Service. The fax is on official looking letterhead, identifies the business owner as a non-resident alien and therefore exempt from specific taxes, and asks him to fax personal and business financial information on Form W-8BEN-11 to “protect” his exemption. The form requests passport info, Social Security number, mother’s maiden name, bank account numbers and other personal information.
- In Lansing, Michigan, con artists pretending to represent a reputable local retailer are phoning local businesses offering deals on toner for office machines. Once they hook a victim, they can use his financial information without having to deliver the promised product.
- In the United Kingdom, fraudsters are “hijacking” details of registered companies by filing fake documents with the government’s public registry. The criminals then impersonate the companies and use their names, addresses or other details to order expensive merchandise, arrange business deals or divert mail deliveries.

Sometimes a business will become aware that its name is being used for fraudulent purposes when a customer calls to complain about a rude sales representative or non-delivery of a product. Or the stolen identity may be revealed when a business receives bills for goods and services that it never ordered and that were delivered to another address. Other times the tip-off comes when people call to ask about a non-existent job listing; when a stranger calls to ask about a paycheck they never received; or when the receptionist receives phone calls for an “employee” who does not work there. Any of these could signify that someone is using your business’s good name for fraudulent purposes.

Businesses should take proactive steps to lessen the chances that their good names or financial information fall victim to theft. The BBB recommends advising all employees to:

- Treat unsolicited e-mail or fax requests for financial information or personal data with suspicion. Unsolicited means the e-mail was not initiated by you or another staff member and was not in response to an action taken by an employee.
- Never reply to unsolicited e-mails concerning company bank accounts and do not click on a link within an unsolicited e-mail message.
- Contact the actual business or government agency that is requesting financial information from your business to verify its legitimacy. Use a phone number or Web site that you know to be legitimate.
- Never submit your Social Security number, passwords or PINs via an e-mail message or fax.
- Use anti-virus software and security patches and update them regularly to protect system software.
- Check monthly statements to verify all transactions. Notify your financial institution immediately if you detect any erroneous or suspicious transactions.
- Shred sensitive business financial documents and receipts.
- Clean data from any computers that the business plans to sell or dispose of. It is not enough to delete data from the computer’s memory; use specially designed software programs to totally remove the data.
- Scrutinize bills or invoices for goods or services that the business never ordered. Contact the retailer to find out who ordered the products and where they were delivered.
- Always contact your local Better Business Bureau to check out offers, invoices or other materials that your business receives from questionable entities.