BUSINESS CRIME WATCH

BAY CITY DEPARTMENT OF PUBLIC SAFETY July 2018 EDITION 3, VOLUME 7

Credit card processing "deals" may be scams

If you're in a small business, you probably need a way for people to pay you and ways to lower your costs. Scammers have been working both of those angles, promising businesses that they can save on leases of credit card processing equipment. They've also been promising that businesses can cancel any time. But is that what happens? In a word, no. Businesses can end up paying thousands to lease equipment that would have cost only a few hundred dollars to buy. When the business can't cancel the lease (despite the promises), it can have trouble if it stops paying. Those lease agreements can hold the business owner (or the person who signed the lease) responsible for the debts. And the agreements can require that legal disputes are heard in another state. Some scammers have even pretended to be the business's *current* card processor – people have been tricked into signing new contracts when they thought they were just updating paperwork.

To avoid this and other scams against small businesses:

- Don't be rushed. Scammers want a quick decision. But you need to read the contract and check out the company.
- Do your research. Search the company's name online with words like "scam" or "complaint."
- Get it in writing. You'll want to see all the terms in writing before you sign. If you don't get them, walk away. If you do sign, be sure to get a copy of the entire document, especially if you sign electronically.

If you own a small business or are part of a non-profit organization, you spend a lot of time and effort making sure the organization works well. But when scammers go after your organization, it can hurt your reputation and your bottom line. Your best protection? Learn the signs of scams that target businesses. Then tell your employees and colleagues what to look for so they can avoid scams.

SCAMMERS' TACTICS

- **Scammers pretend to be someone you trust.** They make themselves seem believable by pretending to be connected with a company you know or a government agency.
- **Scammers create a sense of urgency.** They rush you into making a quick decision before you look into it.
- **Scammers use intimidation and fear.** They tell you that something terrible is about to happen to get you to send a payment before you have a chance to check out their claims.
- **Scammers use untraceable payment methods.** They often want payment through wire transfers, reloadable cards, or gift cards that are nearly impossible to reverse or track.

HOW CAN I PROTECT MY BUSINESS?

- Train Your Employees
- Your best defense is an informed workforce. Explain to your staff how scams happen and share this brochure with them.
- Encourage people to talk with their coworkers if they spot a scam. Scammers often target multiple people in an organization, so an alert from one employee about a scam can help prevent others from being deceived.
- Train employees not to send passwords or sensitive information by email, even if the email seems to come from a manager. Then stick with the program — don't ever ask for sensitive data from employees by email.

Verify Invoices and Payments

- Check all invoices closely. Never pay unless you know the bill is for items that were actually ordered and delivered. Tell your staff to do the same.
- Make sure procedures are clear for approving invoices or expenditures. To reduce the risk of a costly mistake, limit the number of people who are authorized to place orders and pay invoices. Review your procedures to make sure major spending can't be triggered by an unexpected call, email, or invoice.
- Pay attention to how someone asks you to pay. Tell your staff to do the same. If you are asked to pay with a wire transfer, reloadable card, or gift card, you can bet it's a scam.

Be Tech-Savvy

- Don't believe your caller ID. Imposters often fake caller ID information so you'll be more likely to believe them when they claim to be a government agency or a vendor you trust.

- Remember that email addresses and websites that look legitimate are easy for scammers to fake. Stop and think about whether it could be a scam before you click. Scammers even can hack into the social media accounts of people you trust and send you messages that appear to be from them. Don't open attachments or download files from unexpected emails; they may have viruses that can harm your computer.
- Secure your organization's files, passwords, and financial information. For more information about protecting your small business or non-profit organization's computer system, check out the FTC's Small Business Computer Security Basics at FTC.gov/SmallBusiness**.**

Know Who You're Dealing With

- Before doing business with a new company, search the company's name online with the term "scam" or "complaint." Read what others are saying about that company.
- When it comes to products and services for your business, ask for recommendations from other business owners in your community. Positive word-of-mouth from trustworthy people is more reliable than any sales pitch.
- Don't pay for "free" information. You may be able to get truly free business development advice and counseling through programs like **SCORE.org**.

COMMON SCAMS THAT TARGET SMALL BUSINESS

Fake Invoices

Scammers create phony invoices that look like they're for products or services your business uses — maybe office or cleaning supplies or domain name registrations. Scammers hope the person who pays your bills will assume the invoices are for things the company actually ordered. Scammers know that when the invoice is for something critical, like keeping your website up and running, you may pay first and ask questions later. Except it's all fake, and if you pay, your money may be gone.

Unordered Office Supplies and Other Products

Someone calls to confirm an existing order of office supplies or other merchandise, verify an address, or offer a free catalog or sample. If you say yes, then comes the surprise — unordered merchandise arrives at your doorstep, followed by high-pressure demands to pay for it. If you don't pay, the scammer may even play back a tape of the earlier call as "proof" that the order was placed. Keep in mind that if you receive merchandise you didn't order, you have a legal right to keep it for free.

Directory Listing and Advertising Scams

Con artists try to fool you into paying for nonexistent advertising or a listing in a nonexistent directory. They often pretend to be from the Yellow Pages. They may ask you to provide contact information for a "free" listing or say the call is simply to confirm your information for an existing order. Later, you'll get a big bill, and the scammers may use details or even a recording of the earlier call to pressure you to pay.

Utility Company Imposter Scams

Scammers pretend to call from a gas, electric, or water company saying your service is about to be interrupted. They want to scare you into believing a late bill must be paid immediately, often with a wire transfer or a reloadable card or gift card. Their timing is often carefully planned to create the greatest urgency — like just before the dinner rush in a restaurant.

Government Agency Imposter Scams

Scammers impersonate government agents, threatening to suspend business licenses, impose fines, or even take legal action if you don't pay taxes, renew government licenses or registrations, or other fees. Some businesses have been scared into buying workplace compliance posters that are available for free from the U.S. Department of Labor. Others have been tricked into paying to receive nonexistent business grants from fake government programs. Businesses have received letters, often claiming to be from the U.S. Patent and Trademark Office, warning that they'll lose their trademarks if they don't pay a fee immediately, or saying that they owe money for additional registration services.

Tech Support Scams

Tech support scams start with a call or an alarming pop-up message pretending to be from a well-known company, telling you there is a problem with your computer security. Their goal is to get your money, access to your computer, or both. They may ask you to pay them to fix a problem you don't really have, or enroll your business in a nonexistent or useless computer maintenance program. They may even access sensitive data like passwords, customer records, or credit card information.

Social Engineering, Phishing, and Ransomware

Cyber scammers can trick employees into giving up confidential or sensitive information, such as passwords or bank information. It often starts with a phishing email, social media contact, or a call that seems to come from a trusted source, such as a supervisor or other senior employee, but creates urgency or fear. Scammers tell employees to wire money or provide access to sensitive company information. Other emails may look like routine password update requests or other automated messages but are actually attempts to steal your information. Scammers also can use malware to lock organizations' files and hold them for ransom.

Business Promotion and Coaching Scams

Some scammers sell bogus business coaching and internet promotion services. Using fake testimonials, videos, seminar presentations, and telemarketing calls, the scammers falsely promise amazing results and exclusive market research for people who pay their fees. They also may lure you in with low initial costs, only to ask for thousands of dollars later. In reality, the scammers leave budding entrepreneurs without the help they sought and with thousands of dollars of debt.

Changing Online Reviews

Some scammers claim they can replace negative reviews of your product or service, or boost your scores on ratings sites. However, posting fake reviews is illegal. FTC guidelines say endorsements — including reviews — must reflect the honest opinions and experiences of the endorser.

Credit Card Processing and Equipment Leasing Scams

Scammers know that small businesses are looking for ways to reduce costs. Some deceptively promise lower rates for processing credit card transactions, or better deals on equipment leasing. These scammers resort to fine print, half-truths, and flat-out lies to get a business owner's signature on a contract. Some

unscrupulous sales agents ask business owners to sign documents that still have key terms left blank. Don't do it. Others have been known to change terms after the fact. If a sales person refuses to give you copies of all documents right then and there — or tries to put you off with a promise to send them later — that could be a sign that you're dealing with a scammer.

Fake Check Scams

Fake check scams happen when a scammer overpays with a check and asks you to wire the extra money to a third party. Scammers always have a good story to explain the overpayment — they're stuck out of the country, they need you to cover taxes or fees, you'll need to buy supplies, or something else. By the time the bank discovers you've deposited a bad check, the scammer already has the money you sent them, and you're stuck repaying the bank. This can happen even after the funds are made available in your account and the bank has told you the check has "cleared."

Bay City Bridge, Traffic and Operations Study

OHM Associates is conducting a study to determine the feasibility and impacts for different alternatives for the City's bridge operations at Independence and Liberty Bridges.

During the study, there will be a public meeting to gather public input and answer questions, along with a website that will be available for public input, surveys and general information. There will be updates on the study on the website, Status and Information and to the Commission.

The study will take into account costs of repairing and maintaining the bridges in their current configuration; as well as explore options to limit use or remove a bridge. It will also include an investigation into impacts to traffic patterns and operations, economic impacts to local businesses, social impacts, and environmental impacts. The findings and recommendations will be presented at a Commission Meeting in November. All impacts and findings will be included in the final report; as well as online input, surveys and input from the public meeting with responses. The final report will be available for public viewing at City Hall after the study is complete.

The City has submitted an application for a grant from the East Michigan Council of Governments to help fund the study.

Reminder with the Fourth of July holiday fast approaching, some of our customers will experience a service delay.

July 4th Independence Day (Wednesday) Office Closed 1 day delay

Crews working Thursday, July 5th thru Saturday, July 7th

Boards and Committees

- Charter Commission Meeting
  July 10, 2018, 7:00 PM - 8:30 PM @ Conference Room 306
- Zoning Board of Appeals
  July 10, 2018, 7:00 PM - 8:00 PM @ Commission Chambers
- Historic District Commission
  July 11, 2018, 5:30 PM - 6:30 PM @ Commission Chambers
- Planning Commission
  July 18, 2018, 7:00 PM - 8:00 PM @ Commission Chambers
- Charter Commission Meeting
  July 24, 2018, 7:00 PM - 8:30 PM @ Conference Room 306
- Historic District Commission
  July 25, 2018, 5:30 PM - 6:30 PM @ Commission Chambers

City Commission

- Finance Policy Meeting 7/2/18 @ 6:30
  July 2, 2018, 6:30 PM - 7:30 PM @ Commission Chambers
- City Commission Meeting
  July 2, 2018, 7:30 PM - 8:30 PM
- Finance Policy Meeting
  July 16, 2018, 6:30 PM - 7:30 PM
- City Commission Meeting
  July 16, 2018, 7:30 PM - 8:30 PM

Community Development Block Grant/CDCs

- South End Citizens District Council
  July 19, 2018, 7:00 PM - 8:00 PM @ Bay County Child & Senior Center
- Northeast Citizens District Council
  July 25, 2018, 6:00 PM - 7:00 PM @ Conference Room 317

Special / Community Events

- Downtown Bay City Farmers Market
  July 5, 2018, 10:00 AM - 4:00 PM @ 800 block of Jefferson Avenue at Center Avenue
- Bay City Fireworks Festival
  July 5, 2018, 10:00 PM - 11:00 PM @ Veterans Memorial Park
  Veterans Memorial Park and Wenonah Park
- Bay City Fireworks Festival
  July 6, 2018, 10:00 PM - 11:00 PM @ Veterans Memorial Park
  Veterans Memorial Park and Wenonah Park
- Bay City Fireworks Festival
  July 7, 2018, 10:00 PM - 11:00 PM @ Veterans Memorial Park
  Veterans Memorial Park and Wenonah Park
- Downtown Bay City Farmers Market
  July 12, 2018, 10:00 AM - 4:00 PM @ 800 block of Jefferson Avenue at Center Avenue
- Cool City Car Show
  July 13, 2018, 6:00 PM - 10:00 PM @ Midland Street

- Cool City Car Show
  July 14, 2018, 8:00 AM - 4:00 PM @ Downtown Streets
- Downtown Bay City Farmers Market
  July 19, 2018, 10:00 AM - 4:00 PM @ 800 block of Jefferson Avenue at Center Avenue
- Downtown Bay City Farmers Market
  July 26, 2018, 10:00 AM - 4:00 PM @ 800 block of Jefferson Avenue at Center Avenue
- Blues Traveler Concert
  July 28, 2018, 4:00 PM - 11:00 PM @ Wenonah Park

National Night Out 2018

Don’t forget to register your organization for National Night Out

National Night Out is an annual community-building campaign that promotes police-community partnerships and neighborhood camaraderie to make our neighborhoods safer, better places to live. Together, we are making that happen. On Tuesday August 7th from 5pm – 8pm neighbors throughout Bay City and across the nation are asked to lock their doors, turn on their front porch lights and spend the evening outside with neighbors and law enforcement.

The Bay City Department of Public Safety will be hosting our National Night Out event at Uptown Bay City. This event will have games and prizes for the kids, numerous public safety vehicles, non-profit organizations, music, a bounce houses, food, games and a cook off. We would like to invite your organization to come join us. You are welcome to set up a booth or table to provide information about your organization, sponsor an event, or donate a prize.

2018 National Night Out Registration Form

Please send your reservation form to communitypolicing@baycitymi.org You may also mail your reservation to the Bay City Department of Public Safety, Community Policing Unit, 501 3rd Street, Bay City, MI 48708.

The 2018 location will once again be at Uptown Bay City, just north of Dow Corning. Entrance is off of Main Street. You may pull into the Dow Corning parking lot to unload. Vendor parking will then be located on Saginaw Street between 10th & 11th. This year's event will be located outside on the grassy area just to the north of Dow Corning (look for the Dow tent). Please indicate below if you need a power outlet. Bring a table, chairs and pop up tent if needed.

Please include the following:

Contact Person _____

Organization _____

Address _____

Phone Number _____

Email Address _____

Amount of space needed if more than a 10 x 10 area: _____

_____

Additional Info_____

Power outlet: YES or NO

National Night Out will be held on Tuesday August 7th from 5pm – 8pm. Set up will be from 3pm – 5pm, You may arrive earlier if more time is needed. The event will be held rain or shine.

We look forward to your participation in America's National Night Out Against Crime! If you have any questions, please feel free to contact us.

Officer Leslie Darrow
ldarrow@baycitymi.org

Officer Eric Sporman
esporman@baycitymi.org