Special Communication to City of Burlington Emergency Operations Center and Mayor Regarding COVID-19

To: Burlington Resource & Recovery Center, Brian Lowe, Luke McGowan

From: Barbara Shatara of City Analytics Team

RE: COVID-19 Scam Information for RRC Website

Date: April 11, 2020, 12:30pm

Key Messages:

- Despite widespread attention on the rise of scams and fraud related to the COVID-19 pandemic and subsequent Federal aid packages, the US Federal Trade Commission reported it has received more than **15,000 fraud complaints related to the coronavirus outbreak**, and **consumers have lost nearly $12 million to COVID-19 scams**, since the beginning of the year.
- Scams that have been reported to-date include criminals impersonating the Social Security Administration, IRS, FBI, WHO, CDC, U.S. Dept. of Health & Human Services, Medicare, student loan agencies, well-known charities, and even local-assistance initiatives or employers. Scams often center around **coronavirus stimulus checks, other forms of aid, coronavirus testing and treatment, goods and services to protect yourself/your home, and charitable donations**.
- In general, to protect yourself from scams during this time, you should **beware of unsolicited calls or emails, don't give out personal information, be aware of scare tactics** including demands for immediate action or make threatening statements, and **don't open email attachments or talk to callers on suspicious phone calls.** Always do your research using one of the enclosed resources, and take steps to verify whether the contact was a scam.
- Enclosed is a summary of known COVID-19 scams reported by federal and state agencies, as well as information about how to protect yourself. In particular, the FTC website is one of the most comprehensive websites on scams and fraud in the U.S.
- The Office of the Vermont Attorney General's COVID-19 website is another helpful resource that lists scams and general tips. It is important for consumers to report a scam, price gouging, or other consumer concerns tor attempts at fraud to Vermont's Consumer Protection Agency at AGO.CAP@vermont.gov or 1-800-649-2424.
- Other scams are targeted directly at older adults and others who may be especially vulnerable during this pandemic. AARP Coronavirus Scam list includes detailed information about these targeted scams, and AgeWell's Coronavirus and Older Vermonters webpage has a Trusted Resources section.

Important Note Regarding this Document: *The coronavirus pandemic, and local, state and federal guidance/orders regarding this pandemic, are rapidly evolving. Information contained in this memo is presumed to be accurate and reflective of the situation as of the date and time noted above. Information in this memo is offered as review of actions, events, case studies, and data based on specific requests of and research by the Analytics Team. The original audience for this document was the Mayor and members of the City's Emergency Operations Center. These resources are being made available in the event that they may be informative for other Vermont communities.*

Key Resources

These are key links to find out more information about or to report scams:

- Federal Trade Commission Consumer Information - Scams
- FCC List of COVID19 Scams and Scam Glossary
- U.S. Department of Justice National Center for Disaster Fraud COVID19 and Disaster Fraud Line
- Office of the Vermont Attorney General – COVID19 Scams
- State of Vermont Department of Financial Regulation
- State of Vermont Department of Taxes Report Identity Theft or Fraud
- AARP Coronavirus Scam list
- University of Vermont Consumer Assistance Program

Summary of Available Information on Coronavirus Scams and Frauds

Coronavirus Stimulus Checks Scam

These scams exploit confusion over how Stimulus checks will be distributed. Both individuals and tax preparers are being targeted. These scams may take the form of fake checks sent in the mail, or calls, texts or emails asking you to access or verify your information to ensure you get your payment. Here are things you should know to protect yourself and/or your clients:

- **It's *not* the IRS or VT Dept of Taxes calling, texting, or emailing.** Scammers send official-looking messages – including postcards with a password to be used online to "access" or "verify" your payment or direct deposit information. It is important to always remember that neither the IRS and the VT Dept. Of Taxes will not contact you to collect your personal information or bank account.
- **Checks are *not* in the mail – yet.** Reports say that paper checks – for people without direct deposit – will start arriving in May at the earliest. So, if you get an economic impact payment, stimulus, or relief check before then, or you get a check when you're expecting a direct deposit, it's a scam.
- **No one has early access to this money.** Anyone that claims to is a scammer. The timeline for this process is not exact, but it looks like funds will start going out in the next few weeks. Scammers are using the lack of detail to try to trick people into giving their personal information and money.
- **The IRS will *not* send you an overpayment and make you send the money back in cash, gift cards, or through a money transfer.** If you get an official-looking check for more than what you were expecting – say, for $3,000 – the next call you're likely to get is from a scammer. They'll tell you to keep your $1,200 payment, and return the rest by sending cash, gift cards, or money transfers.
- **To set up direct deposit of your check, communicate only with the IRS at irs.gov/coronavirus.** And you only need to do this if you **didn't** give the IRS your bank information on your 2018 or 2019 return. In the coming weeks, the IRS will be setting up an online form available through irs.gov/coronavirus. But nowhere else, and never in response to an email, text, or call.

Important Note Regarding this Document: *The coronavirus pandemic, and local, state and federal guidance/orders regarding this pandemic, are rapidly evolving. Information contained in this memo is presumed to be accurate and reflective of the situation as of the date and time noted above. Information in this memo is offered as review of actions, events, case studies, and data based on specific requests of and research by the Analytics Team. The original audience for this document was the Mayor and members of the City's Emergency Operations Center. These resources are being made available in the event that they may be informative for other Vermont communities.*

Phone Call Scams

- Fake Social Security Administration robocalls, including false reporting of suspicious use of an individual's social security number (SSN)
- Fake COVID 19 Treatment and Testing for Medicare Clients, including calls, texts or emails indicating free or reduced price COVID-19 testing for Medicare recipients, or calls hawking cures or treatments to reduce COVID-19 symptoms or susceptibility.
- Test Kit Phone Scam: One pernicious version of this scam is targeting higher risk individuals with diabetes, offering a free COVID-19 testing kit along with a free diabetic monitor.
- COVID-19 themed work-from-home opportunities, student loan repayment plans, and debt consolidation offers. Consumers aren't the only target. Small businesses are also getting scam calls about virus-related funding or loans and online listing verification.
- Robocalls to offer HVAC duct cleaning as a way to "protect" your home and family from the virus.
- Scammers call or fax, saying the federal government requires posters to be posted in a visible location at their business, or declare that the federal government has new requirements that must be followed due the pandemic and that businesses need to pay a fee to fulfill such requirement.

- *What to do*:
    - Hang up. Don't press any numbers. The recording might say that pressing a number will let you speak to a live operator or remove you from their call list, but it might lead to more robocalls, instead.
    - Consider using a call blocking app or device. You also can ask your phone provider if it has call-blocking tools. To learn more, go to ftc.gov/calls.
    - Report the call. Report robocalls at ftc.gov/complaint.

Fake emails, texts and phishing

Scammers use fake emails or texts to procure valuable personal information — like account numbers, Social Security numbers, or your login IDs and passwords. They use your information to steal your money, your identity, or both. They also use phishing emails to get access to your computer or network. If you click on a link, they can install ransomware or other programs that can lock you out of your data. Scammers often use familiar company names or pretend to be someone you know. Known examples include:

- Fake FCC Financial Care Center texts offering $30,000 in COVID-19 relief. There is no FCC program to provide relief funds to consumers.
- Text message scam impersonating the U.S. Department of Health and Human Services informs recipients that they must take a "mandatory online COVID-19 test" using the included link.
- Beware of fake healthcare products that supposedly protect or cure you from COVID-19, sell you COVID-19 test kits, or offers you employment selling COVID-19 test kits or cures.
- Imposter scams in which a criminal poses as a company's CEO, manager, or other internal employee to convince employees to wire money; agree to pay fake invoices or solicitations in the guise of a bill; or "verify" an address, when really signing businesses up for services.
- FBI Public Service Announcement warning individuals to watch for emails claiming to be from the CDC or other organizations offering information on the virus. Be wary of websites and apps claiming to track COVID-19 cases worldwide.

Fake Charity Requests

The **World Health Organization** recently issued a warning about criminals posing as WHO or another charity, seeking to take advantage of the pandemic to steal money or sensitive personal information from consumers. Scam involves impersonating a charity, sometimes using a legitimate charity's name or one that sounds similar.

- *What to do:*
    - Use FCC list of organizations to help you research charities, UVM's *CAP Connection* blog post, or verify charities by consulting the Vermont Secretary of State's corporation database or by visiting Charity Navigator.
    - Pay safely by credit card — never by gift card or wire transfer.
    -

Friendly Helper Scam & Undelivered Goods Scam

These involve strangers offering to help pick up groceries or prescriptions, then taking your money, or fake online businesses claiming to offer in-demand products (cleaning products, medical supplies), when in fact, they don't. Related are text message scams that purport to be FedEx delivery updates

- *What to do:*
    - If someone you don't know offers to help, be wary. It's usually safer to find a trusted friend or neighbor or arrange a delivery with a well-known company.
    - Use an established delivery service, or order directly from the store. Many grocery stores and pharmacies are offering contactless delivery.
    - If you need additional help for yourself or a loved one, the Eldercare Locator, a public service of the U.S. Administration on Aging, can connect you to services for older adults and their families. You can also call 1-800-677-1116.
    - Check out the seller by searching online for the person or company's name, phone number and email address, plus words like "review," "complaint" or "scam".

Other Sources & Resources

1. *Vermont AG Warns Of Coronavirus Price Gouging, Hoarding & Scams.* Vermont Edition. March 26, 2020.
2. Norton AntiVirus Website How to Protect Yourself from COVID19 Phishing Scams has examples of phishing emails.
3. No, Red Cross Is Not Offering Coronavirus Home Tests. by Bethania Palma. Snopes. Published March 18, 2020. Updated March 19, 2020.
4. *Another Thing to Fear Out There: Coronavirus Scammers.* by Sharon LaFraniere and Chris Hamby. New York Times. April 5, 2020.
5. *How consumers can protect themselves from coronavirus scams* by Julianne Ross. CNN Underscored. April 7, 2020.
6. Coronavirus stimulus scams are here. By Rae Hodge. C/net. April 9, 2020 10:26 a.m.
7. Coronavirus scams have cost consumers nearly $12 million, FTC says. by Carrie Mihalcik. C/net. April 10, 2020 7:43 am.

Important Note Regarding this Document: *The coronavirus pandemic, and local, state and federal guidance/orders regarding this pandemic, are rapidly evolving. Information contained in this memo is presumed to be accurate and reflective of the situation as of the date and time noted above. Information in this memo is offered as review of actions, events, case studies, and data based on specific requests of and research by the Analytics Team. The original audience for this document was the Mayor and members of the City's Emergency Operations Center. These resources are being made available in the event that they may be informative for other Vermont communities.*