VERMONT
DEPARTMENT OF FINANCIAL REGULATION
89 Main Street, Montpelier, VT 05620 - 3101
(p) 802-828-3301 | http://www.dfr.vermont.gov/

DFR Encourages Vermonters to be Knowledgeable About Cryptocurrencies to Avoid Risks and Scams

Investor Alert: August 23, 2021

The Vermont Department of Financial Regulation (DFR) is reporting a spike in cryptocurrency-related scams. Over the last month, DFR has received complaints from Vermonters who collectively reported losing over $1 million to cryptocurrency scams. Before you use, send, or invest in cryptocurrencies, make sure you know what makes cryptocurrencies different from other types of payment methods and investments and know how to spot cryptocurrency scams.

What Are Cryptocurrencies and Why Are They Risky?

Cryptocurrencies are digital assets created by companies or individuals that take the form of a virtual coin or token. Bitcoin and Ethereum are the most widely known cryptocurrencies, but there are many others. Interest in cryptocurrencies is increasing among Vermonters; however, it is vital to know that cryptocurrencies and related investment products are not functional equivalents of traditional banking, securities, or insurance investment products.

Cryptocurrencies are a highly speculative and risky investments. Profits or losses are impossible to predict. Profits are not guaranteed, even when presented as "interest." Cryptocurrency values are highly volatile, making them unsuitable for most investors looking to meet savings or retirement goals. Investors should never speculate in cryptocurrencies with money they cannot afford to lose.

Cryptocurrencies are stored in a digital wallet, which may be online, on your phone or computer, or on an external hard drive. If something unexpected happens to your digital wallet — your account is hacked, you send cryptocurrency to a scammer, you lose your password, or your digital wallet is stolen or compromised — it may be impossible to recover your funds. Digital wallets are not insured by the government, like U.S. dollars in a bank account. If a company is storing your cryptocurrency, and the company goes out of business or is hacked, you may never get your money back.

When you pay with or send cryptocurrency, the transaction is irreversible. Credit cards, debit cards, and traditional financial institutions have legal protections if something goes wrong, and processes to help get your money back. Cryptocurrency transactions lack these protections. If you send or transfer your cryptocurrency to the wrong person – whether by accident or because a scammer or hacker steals your funds - you are unlikely to recover your cryptocurrency. These qualities make cryptocurrencies an irresistible target for criminals.

Common Cryptocurrency Scams

Cryptocurrency scams come in countless varieties. Criminals are always finding new ways to steal your money using cryptocurrencies. Here are some common scams to watch out for.

Cryptocurrency Payments. ***Anyone who says you have to pay by cryptocurrency is probably a scammer***. According to the Federal Trade Commission, this is a "sure sign of a scam." If someone asks to be paid in cryptocurrency or offers a discount or reward for using cryptocurrency, consumers should be on high alert.

"Spoofing" - Fake Emails, Texts, and Websites Pretending to be Trusted Companies. Cybercriminals often imitate the branding, appearance, and function of emails and text messages from well-known and trusted companies. These messages may try to trick you into downloading malicious software or viruses, entering your username or password into a fake website, or initiating a cryptocurrency transfer to a scammer pretending to be a trusted business.

Spoofing scams often target concerns about security or offer opportunities or services that are unavailable to the general public. Spoofing scams have included everything from fake technical support messages, to failed transaction notifications, to notices of unauthorized login attempts, to invitations to transfer cryptocurrency to an upgraded platform for professional cryptocurrency traders.

- Always look at the actual email address (not the screenname) that an email comes from. If it isn't from exactly the website it claims to be from (with no extra characters or words), that is a red flag signaling danger.

- Never click on links in emails or texts for important websites and accounts, like cryptocurrency exchange accounts and other financial accounts. And never blindly click on email or text web links for any site. Hover over the link with your cursor and the web browser will show you the real URL in the status bar. Carefully review for website addresses that don't match the site it claims to be for (with no extra characters or words).

- ***Never download attachments or click on links in suspicious emails or texts. If you are not sure if an email or text is legitimate, do not click on links or download attachments.*** If you decide to contact a company to verify the authenticity of a suspicious email or text, avoid using contact information supplied in the email or text itself.

Phishing Emails. Phishing emails targeting cryptocurrency users come in many other forms beyond spoofing. A common scam involves a person purportedly sending you their digital wallet backup file and private key and asking you to send their bitcoin to another wallet address. This scam appeals to the victim's greed, tempting them to take the money and run. But the wallet file actually contains an executable program that will make off with your cryptocurrency. Never download an attachment from an unsolicited email.

Investment and Business Opportunity Scams. Cryptocurrency-related investment schemes and business opportunities are another favorite tool of scammers. These so-called "opportunities" and "investments" often sound too good to be true. Investors should be especially wary of anyone promising guaranteed returns, free money, or touting large gains with little risk.

Some common investment scams include:

- Promises that you can earn lots of money in a short time.
- Unregistered securities offerings, including so-called ICOs selling new tokens or cryptocurrencies and companies promising to pay interest on cryptocurrency loans or deposits.
- Requirements that you pay in cryptocurrency for the right to recruit others into a program. If you do, they say you'll get recruitment rewards paid in cryptocurrency. The more cryptocurrency you pay, the more money they promise you'll make. These are false promises.
- Unsolicited offers from supposed "investment managers." These scammers say they can help you grow your money if you give them the cryptocurrency you've bought. The scammers may promise to invest, lend, or sell your cryptocurrency to generate profits (often claiming to use new technology that guarantees high profits and low risk). Often, these are little more than Ponzi schemes.
- Investment managers that require you to pay significant fees to withdraw your money or cryptocurrency. This is a ploy to steal even more of your money.
- Unsolicited job offers to help recruit cryptocurrency investors, sell cryptocurrency, mine cryptocurrency, or help with converting cash into cryptocurrencies.

Consumers and investors can find additional information about cryptocurrency scams and frauds online from the FTC.

If you or someone you know have encountered a cryptocurrency scam in Vermont, report it. Use the Vermont Attorney General's online scam reporting form for the Consumer Assistance Program.

Avoid Unlicensed Cryptocurrency Exchanges and Sellers

Vermonters who decide, after considering the risks above, to purchase, trade, or use cryptocurrencies should only do business with companies that hold a Vermont money transmitter license from the DFR. Although dealing with a licensed entity does not eliminate the inherent risks of cryptocurrencies, licensed companies must comply with anti-money

laundering requirements, report to regulators, and submit to criminal background checks for officers, directors, and control persons.

Vermonters should always avoid unlicensed cryptocurrency sellers and exchanges. It is illegal to engage in the business of selling or exchanging cryptocurrency in Vermont without a license. If a company is doing business without the required license, this is a red flag signaling danger.

Consumers can check whether a cryptocurrency seller or exchange is licensed as a money transmitter in Vermont on the DFR website. Consumers can report unlicensed cryptocurrency sellers and exchanges by contacting the DFR Banking Division at dfr.bnkconsumer@vermont.gov.

Unregistered Securities Offerings

In certain cases, cryptocurrencies and cryptocurrency-related investment opportunities may involve securities. If the securities laws apply, an issuer must register the offer and sale with regulators unless a valid exemption applies. The registration requirements ensure that investors receive proper disclosure of material information and that investments are subject to regulatory scrutiny to protect investors.

Unregistered offerings and sales of cryptocurrency securities are a favorite tool of scammers and fraudsters. Investors should be especially cautious of so-called initial coin offerings (ICOs) and initial exchange offerings (IEOs), as well as cryptocurrency interest accounts and cryptocurrency-related investment opportunities, such as schemes that claim to generate interest or returns by investing, trading, or making loans using investors' cryptocurrencies. The U.S. Securities and Exchange Commission has published many resources to help investors better understand these complex topics.

Always beware of any investment opportunity that sounds too good to be true. Before making any financial decisions, ask questions, do your homework, and contact the DFR. You can file a complaint or ask a question through our website.