FinCEN ALERT

FIN-2024-Alert005 **December 18, 2024**

FinCEN Alert on Fraud Schemes Abusing FinCEN's Name, Insignia, and Authorities for Financial Gain

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this alert by including the key term **"FIN-2024-FINCENSCAMS"** in SAR field 2 (Filing Institution Note to FinCEN) and the narrative. Financial institutions should also select SAR field 34(z) (Fraud – Other) and include any other relevant terms, including "**BOI Scam**," "**MSB Scam**," and/or "**FinCEN Imposter Scam**" in the text box, as applicable.

The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this alert to raise awareness of fraud schemes abusing FinCEN's name, insignia,[1] and authorities for financial gain. These FinCEN-specific fraud schemes include scams that exploit beneficial ownership information (BOI) reporting;[2] misuse FinCEN's Money Services Business (MSB) Registration tool;[3] or involve the impersonation of, or misrepresent affiliation with, FinCEN and its employees.[4] These schemes are the latest evolution of scams impacting FinCEN and its stakeholders.[5]

FinCEN reminds financial institutions to be vigilant in identifying such schemes, which seek to solicit money or personal information from the public, and to report suspicious activity related to these schemes to FinCEN. FinCEN further encourages financial institutions[6] to urge their customers to be equally vigilant in identifying and avoiding these and similar government imposter scams.

1. *See* FinCEN, Insignia.
2. In 2021, Congress enacted the bipartisan Corporate Transparency Act (CTA) to curb illicit finance. For more information, *see* FinCEN, Beneficial Ownership Information webpage. On Tuesday, December 3, 2024, in the case of *Texas Top Cop Shop, Inc., et al. v. Garland, et al.*, No. 4:24-cv-00478 (E.D. Tex.), a federal district court in the Eastern District of Texas, Sherman Division, issued an order granting a nationwide preliminary injunction that: (1) enjoins the CTA, including enforcement of that statute and regulations implementing its BOI reporting requirements, and, specifically, (2) stays all deadlines to comply with the CTA's reporting requirements. The Department of Justice, on behalf of Treasury, filed a Notice of Appeal on December 5, 2024. For more information on this case and the impact of this ongoing litigation, please see FinCEN's website, *available at:* https://fincen.gov/boi.
3. *See* FinCEN, MSB Registrant Search. The MSB Registrant Search Page contains entities that have registered as MSBs pursuant to the Bank Secrecy Act's (BSA) implementing regulations at 31 CFR § 1022.380.
4. Government imposter scams are a type of fraud in which scammers impersonate Federal, state, or local government agencies or personnel to perpetrate fraud. According to the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3), losses from government imposter scams increased by 63 percent in 2023 with over 14,000 victims reporting nearly $400 million dollars in losses in that timeframe. *See* FBI IC3, "2023 Internet Crime Report" (Dec. 12, 2023), p. 15. For additional information on government imposter scams *see* Federal Trade Commission (FTC), "How to Avoid a Government Impersonation Scam" (Nov. 2023). *See also* Treasury Office of Inspector General (OIG), Prohibition Against Misuse of Treasury Names, Terms, Symbols, Stationery, Etc.
5. FinCEN has previously notified financial institutions and the public about scams exploiting its name. *See, e.g.*, FinCEN, FinCEN Reminds the Public to be Wary of Fraudulent Correspondence and Phone Calls ("FinCEN Scam Reminder"). These schemes may constitute wire or mail fraud, conviction of which may result in a term of imprisonment of up to 20 years and a fine of up to $250,000.
6. *See* 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).

Consistent with FinCEN's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) National Priorities, this alert seeks to assist covered institutions in combating fraud.[7] The information contained in this alert is derived from FinCEN's analysis of Bank Secrecy Act (BSA) data, open-source reporting, consumer reports to FinCEN and other federal agencies, and information provided by law enforcement partners.

Reporting Abuse of FinCEN's Name, Insignia, and Authorities to Law Enforcement

The public is reminded that any solicitations from individuals or entities abusing FinCEN's name, insignia, or authorities, or impersonating a FinCEN employee should be reported to Treasury's Office of Inspector General[8] (OIG) (Report Fraud, Waste, and Abuse) and the Federal Trade Commission (FTC) (ReportFraud.ftc.gov). It is important to file reports as quickly as possible.

Victims of cyber-enabled government imposter scams should file a complaint with the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) and file a report with their nearest FBI field office.[9]

Anyone with knowledge of fraud schemes involving victims who are age 60 or older can call the U.S. Department of Justice's (DOJ) National Elder Fraud Hotline at 833-FRAUD-11 or 833-372-8311, which will help callers identify appropriate reporting agencies, provide information to assist them in reporting, connect callers directly with appropriate agencies, and provide resources and referrals, on a case-by-case basis.

Scam Typologies Associated with the Exploitation of FinCEN's Name, Insignia, and Authorities

Based on a variety of public and U.S. government sources, FinCEN is aware of an increase in scammers exploiting FinCEN's name, insignia, and authorities to target the public in widespread and varied fraud schemes. The fraud typologies described below are not exhaustive, and financial institutions and the public should remain vigilant to new and emerging fraud schemes invoking FinCEN or the U.S. Department of the Treasury.[10]

Use of Fraudulent BOI Forms and Websites

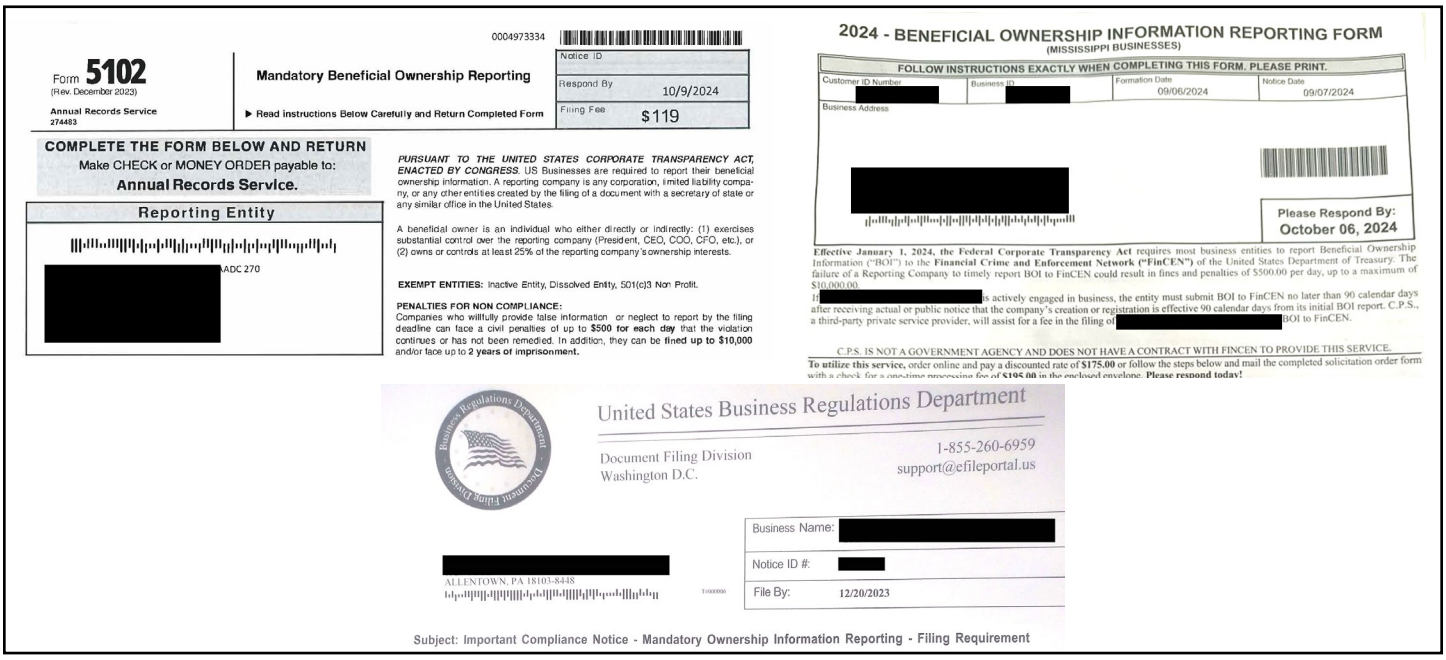
FinCEN is aware of scams targeting companies trying to report BOI to FinCEN. These scammers target companies for the purposes of stealing money or personal information. One scam typology involves scammers convincing companies to pay a "filing fee" to have a third party (i.e., the scammer)

7. Fraud is one of the U.S. AML/CFT National Priorities and continues to be the largest source of illicit proceeds in the United States. *See* FinCEN, "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities" (June 30, 2021); Treasury, "National Money Laundering Risk Assessment" (Feb. 2024).
8. Treasury, About the OIG.
9. According to FBI IC3, "cyber-enabled crime includes any illegal activity that is assisted using cyber-related means. Cyber-enabled crime involves the use of internet technology to communicate false or fraudulent representations to consumers. In addition to websites, emails, and chat rooms, almost all telephone calls utilize internet technology." *See* FBI IC3, Frequently Asked Questions.
10. *See* Treasury OIG, Fraud Alerts.

submit the company's BOI to FinCEN. In these scams, the fraudsters collect money but never file with FinCEN. Scammers may also falsely claim that a filing fee is required when, in fact, there is no filing fee associated with filing BOI.

Scammers may make contact with targeted companies through text message, email, or the U.S. Mail.[11] The scammers may use names strikingly similar to "FinCEN" or pretend to be U.S. government agencies such as a "United States Business Regulations Department" or "Annual Records Service."[12] They may also claim to be legitimate third-party filing companies that file BOI with FinCEN, but who do not actually file.[13] As reported by certain secretary of state offices, scammers have sent companies fictitious beneficial ownership forms such as, for example, a "Form 4022," a "Form 5102," a "2024 Beneficial Ownership Information Reporting Form," or an "Important Compliance Notice," to appear legitimate and demand the companies submit their BOI and pay the filing fee or risk severe fines, penalties, and legal action from FinCEN and the U.S. government.[14] Scammers may direct victims to send the completed fraudulent forms through the U.S. Mail with checks or money orders to pay the filing fees. Or scammers may include links, URLs, or QR codes that direct victims to submit online payments and personal information on fraudulent website domains.[15]

Below are examples of fraudulent BOI reporting forms.



0004973334

Form **5102**
(Rev. December 2023)
Annual Records Service
274483

Mandatory Beneficial Ownership Reporting

▶ Read instructions Below Carefully and Return Completed Form

Notice ID
Respond By 10/9/2024
Filing Fee $119

COMPLETE THE FORM BELOW AND RETURN
Make CHECK or MONEY ORDER payable to:
Annual Records Service.

Reporting Entity

[redacted]
ADC 270

PURSUANT TO THE UNITED STATES CORPORATE TRANSPARENCY ACT, ENACTED BY CONGRESS, US Businesses are required to report their beneficial ownership information. A reporting company is any corporation, limited liability company, or any other entities created by the filing of a document with a secretary of state or any similar office in the United States.

A beneficial owner is an individual who either directly or indirectly: (1) exercises substantial control over the reporting company (President, CEO, COO, CFO, etc.), or (2) owns or controls at least 25% of the reporting company's ownership interests.

EXEMPT ENTITIES: Inactive Entity, Dissolved Entity, 501(c)3 Non Profit.

PENALTIES FOR NON COMPLIANCE:
Companies who willfully provide false information or neglect to report by the filing deadline can face a civil penalties of up to **$500 for each day** that the violation continues or has not been remedied. In addition, they can be **fined up to $10,000** and/or face up to **2 years of imprisonment.**

2024 - BENEFICIAL OWNERSHIP INFORMATION REPORTING FORM
(MISSISSIPPI BUSINESSES)

FOLLOW INSTRUCTIONS EXACTLY WHEN COMPLETING THIS FORM. PLEASE PRINT.

Customer ID Number	Business ID	Formation Date	Notice Date
[redacted]	[redacted]	09/06/2024	09/07/2024

Business Address

[redacted]

Please Respond By:
October 06, 2024

Effective January 1, 2024, the Federal Corporate Transparency Act requires most business entities to report Beneficial Ownership Information ("BOI") to the **Financial Crime and Enforcement Network ("FinCEN")** of the United States Department of Treasury. The failure of a Reporting Company to timely report BOI to FinCEN could result in fines and penalties of $500.00 per day, up to a maximum of $10,000.00.

If [redacted] is actively engaged in business, the entity must submit BOI to FinCEN no later than 90 calendar days after receiving actual or public notice that the company's creation or registration is effective 90 calendar days from its initial BOI report. C.P.S., a third-party private service provider, will assist for a fee in the filing of [redacted] BOI to FinCEN.

C.P.S. IS NOT A GOVERNMENT AGENCY AND DOES NOT HAVE A CONTRACT WITH FINCEN TO PROVIDE THIS SERVICE.
To utilize this service, order online and pay a discounted rate of **$175.00** or follow the steps below and mail the completed solicitation order form with a check for a one-time processing fee of **$195.00** in the enclosed envelope. **Please respond today!**

United States Business Regulations Department

Document Filing Division
Washington D.C.

1-855-260-6959
support@efileportal.us

[redacted]
ALLENTOWN, PA 18103-8448

Business Name: [redacted]
Notice ID #: [redacted]
File By: 12/20/2023

Subject: Important Compliance Notice - Mandatory Ownership Information Reporting - Filing Requirement

11. "U.S. Mail" is a registered trademark of the United States Postal Service and includes all mail distributed and delivered through and by the Postal Service. This includes First-Class Mail such as mailed letters, cards, or other correspondence.
12. *See, e.g.*, FinCEN, Beneficial Ownership Information; State of Mississippi Secretary of State, BOI Filing Scams Alert; Commonwealth of Pennsylvania Department of State, Business and Charities Scams.
13. *See* FinCEN BOI *Frequently Asked Questions*, Section N for further information related to the use of Third-Party Service Providers. While third-party providers may file BOI with FinCEN, FinCEN does not endorse any specific third-party companies that file BOI on behalf of others. Furthermore, while FinCEN does enable certain companies to file BOI through an Application Programming Interface, this authorization likewise does not constitute endorsement of those companies.
14. *See, e.g.*, Commonwealth of Pennsylvania Department of State posting of fictitious "Form 4022"; "Form 5102"; "2024 Beneficial Ownership Information Reporting Form"; "Important Compliance Notice".
15. *See, e.g.*, FinCEN, Beneficial Ownership Information. *See, e.g.*, Commonwealth of Pennsylvania Department of State posting of fictitious "2024 Beneficial Ownership Information Reporting Form"; "Important Compliance Notice".

Guidance on Avoiding BOI Scams

As of the date of publication of this alert and in light of a recent federal court order, reporting companies are not currently required to file BOI with FinCEN and are not subject to liability if they fail to do so while the order remains in force. However, reporting companies may continue to voluntarily submit BOI reports.[16]

For companies who do wish to file voluntarily, FinCEN reminds the public that filing BOI with FinCEN directly through the BOI E-Filing System is **free**. For companies with simple ownership structures, filing may take 20 minutes or less.

Individuals or entities claiming to be FinCEN or another U.S. government agency that request payment to file BOI are **scams**. A U.S. government agency will **never** ask for money to file BOI.

As highlighted on FinCEN's BOI webpage, individuals and companies should be on the lookout for anything that may indicate that a phone call, letter, or text message is fraudulent. As a reminder:

- There is **no** fee to file BOI directly with FinCEN. FinCEN will **not** contact you demanding you pay money to file.
- Be cautious of any message asking you to click on a URL. Those emails or letters could be fraudulent. Do not click on any links or open attachments from a sender you do not recognize.
- Be cautious of any message, by email or over the phone, regarding BOI filing or purported penalties. **At this time, companies are NOT currently required to file their BOI with FinCEN** and will not be subject to liability if they fail to do so while the preliminary injunction remains in effect. **Any correspondence that threatens penalties is inaccurate**.
- FinCEN will not ask for, and you should not submit, payments via phone, mail, or websites through such outreach.
- Use caution when you receive correspondence from an unknown party. Verify the sender. Never give personal information, including regarding BOI, to anyone unless you trust the other party.

Use of Third Parties for BOI Reporting: Companies that wish to voluntarily report may also choose to pay a third-party filing company or service provider to file BOI on their behalf. FinCEN urges caution when interacting with unknown parties. Verify before sending any money or personal information, especially in response to unsolicited correspondence. Companies should be wary of third parties that use tactics such as exorbitant fees, threats of penalties, or false claims that companies must use a third-party service provider to file BOI given the potential risks that such entities may be fraudulent.

16. For more information on this case and the impact of this ongoing litigation, please see FinCEN's website, *available at:* https://fincen.gov/boi.

Fraudulently Registering as MSBs with FinCEN

FinCEN is also aware of scammers fraudulently registering as MSBs with FinCEN, then using that self-registration to appear legitimate or otherwise gain credibility. With limited exceptions, persons meeting the definition of an MSB are required to register with FinCEN within 180 days after the date on which the MSB is established.[17] Once registered with FinCEN, an MSB is included in a publicly accessible and searchable repository of entities registered with FinCEN as MSBs.[18] The scammers are sometimes part of virtual asset investment scams, including so-called "pig butchering" or "Sha Zhu Pan" fraud schemes.[19] As part of these schemes, scammers may instruct victims to purchase virtual currency via virtual asset service providers (VASPs) and direct victims to send the funds to fraudulent MSBs.

Scammers often submit false information when registering with FinCEN and leverage their subsequent appearance on FinCEN's MSB Registrant Search Page to give the impression of being legitimate.[20] These scams usually involve the improper use of their MSB registration to fraudulently claim the entity is vetted, approved, or licensed by FinCEN, when, in reality, the mere fact of MSB registration does not confer any type of approval. These false claims appear on websites and mobile applications and may be used to further investment scams. Such false claims of being vetted, approved, or licensed by FinCEN also appear in wire news services and on social media platforms like Facebook, X, and Telegram. In some cases, the scammers post copies of their MSB registrations in press releases, on their website, or in messages on social media, or they direct potential victims to FinCEN's MSB Registrant Search Page.[21]

Fraudsters claim that their MSBs are "approved by FinCEN." These claims are false, as registration with FinCEN as an MSB does not constitute FinCEN's "approval" of the MSB's business. These fraudsters may accompany such false claims with sweeping statements that they are "compliant with all regulations," or are "global leaders in financial services" in an effort to convince victims that they can safely invest in risk-free and high-return virtual currencies and other digital assets. Companies making such claims about MSB registrations or supposed "licenses" are often seeking to defraud investors.[22]

17. *See* 31 CFR §§ 1010.100(ff), 1022.380.
18. *See* MSB Registrant Search, *supra* note 3.
19. *See* FinCEN, FIN-2023-Alert005, "FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as 'Pig Butchering'" (Sep. 8, 2023); FinCEN Research and Analysis Division Associate Director Dara Daniels, "Statement Before the U.S. House of Representatives Committee on Financial Services for a Hearing Entitled 'Protecting Americans' Savings: Examining the Economics of the Multi-Billion Dollar Romance Confidence Scam Industry'" (Sep. 18, 2024); American Bankers Association, "Crypto Investment Scams" (Sep. 11, 2024); FBI IC3, "The FBI Warns of a Spike in Cryptocurrency Investment Schemes" (Mar. 14, 2023); United States Secret Service, Cryptocurrency Investment Scams.
20. Based on FinCEN's analysis of select MSB registrations, these fraudulent MSBs generally share the same street addresses and are not licensed as MSBs with U.S. state and territorial financial regulatory authorities where they purport to operate, nor are they compliant with BSA reporting requirements.
21. *See* MSB Registrant Search, *supra* note 3.
22. In similar virtual currency investment schemes, victims have sent payments from savings or retirement accounts at banks, mutual fund companies, or broker-dealers through well-established virtual currency exchangers to ultimately unhosted wallet addresses that the scammers control. *See generally*, FinCEN, FIN-2023-Alert005, "FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as 'Pig Butchering'" (Sep. 8, 2023).

[redacted] Secures MSB License to Enhance Global Compliance

[redacted]

Topic: Company Update Share this Article

NEW YORK, NY / ACCESSWIRE / [redacted] has successfully obtained the Money Services Business (MSB) license from the U.S. Financial Crimes Enforcement Network (FinCEN), marking a significant milestone in the company's quest to enhance compliance and provide users with heightened security and trust.

Financial Crimes Enforcement Network
Department of the Treasury

MSB Registration Status Information

[redacted]

The inclusion of a business on the MSB Registrant Search Web page is not a recommendation, certification of legitimacy, or endorsement of the business by any government agency.

The MSB Registrant Search Web page, which is updated on a weekly basis, contains entities that have registered as Money Services Businesses (MSBs) pursuant to the Bank Secrecy Act (BSA) regulations at 31 CFR 1022.380(a)-(f), administered by the Financial Crimes Enforcement Network (FinCEN).

Information contained on this site has been provided by the MSB registrant. FinCEN does not verify information submitted by the MSB. Information provided on this site reflects only what was provided directly to FinCEN. If an error or incomplete information is detected on this site, the registrant should follow the appropriate instructions for correcting a Registration of Money Services Business (RMSB) form.

MSB Registration Number: [redacted]
Registration Type: Initial Registration
Legal Name: [redacted]
DBA Name:

Image from a news source of an MSB claiming it has obtained a license from FinCEN as proof of its enhanced compliance program. FinCEN does not grant licenses nor endorse MSB compliance programs.

Guidance on Avoiding MSB Registration Scams

FinCEN reminds financial institutions and the public that MSBs are required to register with FinCEN as part of their obligations under the BSA, but that registration with FinCEN and a company's appearance on the MSB Registrant Search Page is **not** a recommendation, certification of legitimacy, or endorsement by FinCEN or any other U.S. government agency of the business.

Further, while MSBs must register with and are regulated by FinCEN, FinCEN does **not** license MSBs to operate in the United States. Any claim that a registration with FinCEN is a recommendation, certification of legitimacy, or endorsement by FinCEN of the business or equates their registration as a license to operate in the United States is false.[23] Any business making such a claim may be part of a scam.

MSBs are also regulated by states or territories, including, with very limited exception, needing to obtain a license for each state or territory (collectively, state) in which an MSB operates. State licensing requirements for MSBs vary by state, but in general, states require MSBs to register with FinCEN as part of their licensing requirements. Information about an MSB's state license and authorization by a state to conduct business can be located via the Nationwide Multistate Licensing System (NMLS) Consumer Access search page.

23. *See* MSB Registrant Search, *supra* note 3.

Penalties for Fraudulent MSB Registration

Complete and accurate MSB registration data is an important way for FinCEN, law enforcement, and other regulators to identify and, when necessary, contact a financial institution for reasons that range from obtaining supervisory information (like an MSB agent list) or to serve legal process.[24] The filing of false or materially incomplete information in connection with the registration of an MSB—including registering an MSB that does not exist—is a violation of the BSA and its implementing regulations and likely other criminal laws.[25] Any person who violates such provisions may face both criminal and civil penalties.[26]

Civil penalties for willful violations may include a $10,289 penalty per day the violation continues.[27] Criminal violations for whoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business, may include fines or imprisonment not more than 5 years per violation, or both.[28] The term "unlicensed money transmitting business" includes a money transmitting business that fails to comply with FinCEN's MSB registration requirements.[29]

Impersonation of FinCEN and Its Employees

Scammers are also using FinCEN's name, insignia, and authorities to impersonate FinCEN and its employees in various government imposter scams.[30] These FinCEN imposter scams generally involve scammers contacting people through spoofed[31] phone calls, text messages, emails, or U.S. Mail. In many cases, these schemes may use stolen personally identifiable information to target and convince the victims that the imposters are legitimate.[32]

For example, scammers contact victims and already know their names, Social Security numbers, and account numbers.[33] Scammers also claim to be FinCEN and demand payments for supposed AML/CFT violations and outstanding debts. As part of these schemes, the scammers provide the victims with fictitious documentation, including documents supposedly from the FinCEN Director or Deputy Director, and threaten the individuals with arrest or seizure of their accounts if they do not send payments. In other cases, scammers impersonate FinCEN and claim that the victims are entitled to a financial grant from the Treasury Department but must first provide their bank account information and make a payment to FinCEN to release the funds.[34] FinCEN reminds financial institutions and

24. *See* 31 CFR 1022.380(d)(1) "A money services business must prepare and maintain a list of its agents."
25. *See* 31 U.S.C. § 5330(a)(4).
26. *See* 31 U.S.C. § 5330(e); 31 CFR 1022.380; 31 CFR 1010.821; and 18 U.S.C. 1960(b)(1)(B).
27. *See* 31 U.S.C. § 5330(e); 31 CFR 1010.821.
28. *See* 18 U.S.C. § 1960(a).
29. *See* 18 U.S.C. § 1960(b)(1)(B).
30. According to the FTC, from November 1, 2023 through October 31, 2024, 1,154 fraud reports were filed with the FTC's Consumer Sentinel Network that mentioned "FinCEN," with reported losses of over $69 million. *See also* Treasury OIG, Fraud Alerts.
31. According to the FBI, "spoofing is when someone disguises an email address, sender name, phone number, or website URL—to convince you that you are interacting with a trusted source." *See generally* FBI, Spoofing and Phishing.
32. *See generally*, FBI IC3, "FBI Warns of the Impersonation of Law Enforcement and Government Officials" (Mar. 7, 2022).
33. *See generally* FinCEN Scam Reminder, *supra* note 5.
34. *Id.*

the public: **FinCEN and its employees will not threaten you by email, call, or text and demand immediate payment for any reason**. FinCEN does not offer grants or collect debts.

In a more recent scheme, scammers associated with a fraudulent MSB sent a fake "FinCEN Alert" to the victims of their virtual asset investment scams through Telegram and other social media platforms. The fraudulent alert claims that victims cannot access their funds on the exchange because "FinCEN has frozen all accounts due to an ongoing AML/CFT investigation." It further claims that all the investors are "potential suspects in FinCEN's AML/CFT investigation" and must pay a "self-certification" fee based on a percentage of their investments so that FinCEN can verify that the funds are legitimate and unfreeze all accounts. To further convince victims to pay the fee, the scammers claim they were also paying a fee to FinCEN and covering part of the costs for all investors. However, as is typical in such scams, despite victims paying the requested fee(s) to scammers, the victims will likely never be able to access their funds. FinCEN reminds financial institutions and the public: **FinCEN does not have authority to freeze assets or block funds transfers and will never request payment from the public as part of any AML/CFT investigation.**

How to Identify a Scam

FinCEN urges caution against any unsolicited messages from individuals or entities claiming to be FinCEN. Scammers may call, email, write, or text members of the public. They may use the name of a person who works at FinCEN or send you something claiming it is from FinCEN. FinCEN is providing these tips below:

FinCEN Does Not:

- Contact members of the general public to request payment by phone, text, email, or mail.
- Send unsolicited email, mail, or text, or contact the public by phone, other than mailings providing general information about beneficial ownership reporting.
- Send members of the public direct invitations to connect on social media platforms.
- Demand immediate payment or ask you to move your money to a safe location by email, call, or text. If someone does that and claims to be doing so on behalf of FinCEN, it is a scam.
- Freeze assets. FinCEN will not contact you about frozen assets or blocked transfers.
- Ask you to pay money to access your funds or prove you are not involved in criminal activity.
- Charge you to file reports directly with FinCEN.
- Ask for (and you should never submit) payments via phone, mail, or websites in response to such outreach. Be cautious of any message, by email or over the phone, regarding penalties.
- Offer grants nor collect debts.

- Approve or endorse any business that has registered as an MSB.[35] Any such claim or similar claims are false and may be part of a scam. You should not trust a company solely because it is listed on FinCEN's MSB Registrant Search Page. A business operating as an MSB is required to register with FinCEN.

FinCEN Does:

- Post official documents on its website, www.fincen.gov. FinCEN-issued Alerts, Advisories, and Notices are published at https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets. FinCEN also posts information through its official channels on various social media platforms to include LinkedIn, X, Facebook, and YouTube.
- Provide free e-Filing portals for FinCEN reports.
- Respond to inquiries sent to our Beneficial Ownership Contact Center by email from noreply.contactcenter@fincen.gov.
- Respond to inquiries sent to our Regulatory Support Section through phone calls and by email from frc@fincen.gov.

If you receive a message from someone claiming to be from FinCEN, you can check to see if it is real by contacting FinCEN directly by submitting an inquiry at www.fincen.gov/contact. FinCEN's Regulatory Support Section will respond to the inquiry by phone or email from frc@fincen.gov on the validity of the message.

Red Flag Indicators for Financial Institutions

FinCEN has identified the following red flag indicators to help detect, prevent, and report potential suspicious activity related to scammers abusing FinCEN's name, insignia, and authorities to perpetrate fraud. Because no single red flag is determinative of illicit or other suspicious activity, financial institutions should consider the surrounding facts and circumstances. This may include, but is not limited to, a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple red flags before determining if a behavior or transaction is suspicious or otherwise indicative of these schemes.

Red Flag Indicators for BOI Reporting Scams

1. A customer intending to file their BOI directly with FinCEN makes an online payment.[36]
2. A customer makes an online payment to file their BOI with a third-party filing company or service provider through a website domain that is registered in a foreign location.

35. In addition to the federal registration process through FinCEN, 49 of 50 states as well as the District of Columbia, the Commonwealth of Puerto Rico, and the U.S. Virgin Islands have MSB licensing requirements. For additional resources on an MSB's state license and authorization by a state or territory to conduct business *see generally* NMLS, Consumer Access.
36. A customer can voluntarily electronically file BOI directly with FinCEN at no cost at https://boiefiling.fincen.gov/.

3. A customer sends a payment to file their BOI through a third-party filing company or service provider with little to no online presence or a name similar to legitimate companies or government entities.

4. A customer uncharacteristically sends a payment to a counterparty and tells the financial institution that the funds must be sent immediately to FinCEN or risk a fine, penalty, or legal action for failure to file their BOI.

Red Flag Indicators for Fraudulent Schemes Involving MSBs

5. A company announces its "license" or "approval" from FinCEN as an MSB via a press release through a news wire service, on its website, or social media.

6. A company has been flagged by a state financial regulator as potentially fraudulent or for having exploited victims in the past.

7. A company is registered as an MSB with FinCEN but is not licensed as an MSB with any U.S. state or territorial financial regulatory authority where they claim to operate.[37]

8. A company with a limited online presence prominently highlights their MSB registration with FinCEN or claims to be licensed by FinCEN alongside unverified testimonials and promotions of risk-free high-investment returns, often on its website, a news wire service, or a social media post.

9. An MSB registered with FinCEN shares a street address with other recently registered MSBs.

10. VASPs or other financial institutions provide a user with a virtual currency deposit address that has been flagged as potentially fraudulent by blockchain explorers or blockchain analytic tools.

11. An MSB claims that its AML Program or "know your customer" policies, procedures, or internal controls have been formally approved or otherwise vetted by FinCEN.

12. An individual or entity claims that their MSB registration with FinCEN is either a "recommendation," "certification of legitimacy," "approval," or "endorsement" by FinCEN, Treasury, or the U.S. government, or any U.S. government official.

13. An individual or entity claims that their MSB registration with FinCEN equates to U.S. government approval to operate in the United States.

14. An MSB suggests that users need to pay an AML-related processing "fee" or a "FinCEN fee" to use its services, including to deposit or withdraw funds from its platform.

37. *See generally* NMLS, Consumer Access.

15 A company is registered as an MSB with the same or very similar name of a large, well-known financial institution that appears to lack an MSB registration requirement, such as a bank, credit union, or broker-dealer, and appears to have no official affiliation with that large, well-known financial institution.

Red Flag Indicators for FinCEN Imposter Schemes

16 A customer sends a payment purportedly to FinCEN or in connection with an apparent penalty owed to FinCEN, with the memo line denoting "tax," "fee," "debt," "prize," "lien," or "grant."

17 A customer uncharacteristically sends payments to a new counterparty and indicates to the financial institution that the funds must be sent immediately to pay FinCEN for a supposed "AML/CFT violation," "outstanding debt," or a "Treasury grant."

18 A customer indicates that they received a phone call, text message, email, or U.S. Mail from FinCEN demanding immediate payment.

19 A customer presents a letter supposedly from the FinCEN Director, Deputy Director, or any other FinCEN or Treasury official requesting immediate payment.

For Further Information

FinCEN's website at www.fincen.gov contains information on how to register for FinCEN Updates. Questions or comments regarding the contents of this alert should be addressed to the FinCEN Regulatory Support Section by submitting an inquiry at www.fincen.gov/contact.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit activity, counter money laundering and the financing of terrorism, and promote national security through strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.