

Reporting malicious wallet addresses

10/25/2024 12:32 am EDT

Users that want to report cryptocurrency fraud or want to report stolen cryptocurrency sometimes want to report the addresses associated with the fraud. Reporting the addresses can be helpful to notify exchanges about questionable or illicit sources of funds, and can warn other potential victims about the fraud. There are roughly 5 types of entities that malicious addresses can be reported to.

1. Blockchain explorers, depending on the cryptocurrency.

Addresses can be reported to public blockchain explorers. For example, for the Ethereum blockchain, you can [report malicious addresses to Etherscan](#). Similar reporting is in place for other blockchains e.g. bscscan for BSC, Tronscan for Tron. However, this is not available for all cryptocurrency. Blockchains like Bitcoin that operate on a UTXO model rather than an account-based model like Ethereum generally do not provide options to flag addresses, and the flagging would become obsolete so quickly as a result of the UTXO model. To report Bitcoin or Litecoin addresses for example, you'll have to use other options.

2. Open source reporting tools like [Chainabuse.com](#)

It's often a good idea to report addresses to free malicious address aggregators like [Chainabuse.com](#) which let's other people publicly know about malicious addresses, free of charge.

3. Professional blockchain forensics software providers

It is standard practice for crypto exchanges to use forensic software monitoring and flagging tools as part of their compliance program. Commonly used tools include those provided by Chainalysis, TRM, and Crystal. Reporting to these tools providers will allow them to mark it in their software, and if their customers receive funds deriving from the marked address, exchanges can elect to flag, review, or even freeze the deposit depending on severity. In all likelihood, you will not be successful if you reach out yourself and make the request as such marking requires ample vetting to ensure it is a legitimate theft or fraud. Instead, consider reaching out to reputable blockchain forensic investigative firms who use multiple forensics tools (like Cryptoforensic Investigators) who can report to the various software providers.

4. Free blockchain forensics software providers

There aren't many decent forensic software options out there, but one such option is [breadcrumbs.app](#). While you can report addresses directly to them, it may not prove all that helpful since exchanges generally don't conduct transaction monitoring with such free tools.

5. Exchanges directly.

There can be instances where it makes sense to report malicious address to exchanges directly, even more so if you know possible exchanges the funds may be sent to (or are actively being sent to). Consider whether or not to seek professional assistance to identify relevant exchanges and contact them.

6. Law enforcement

It is a good idea to report the fraud to law enforcement directly in many cases, along with addresses associated with the fraud. It should be kept in mind however that law enforcement agencies do not keep a database of all the malicious addresses reported to them, as some of the other options do.

7. Private Blockchain Investigative Firms

Reporting fraudulent addresses to a private firms (like our company) can be helpful insofar as those addresses can then be tracked, flagged, to the same types of reporting sources as listed above.
