Q: What evidence should I provide if I want to report a scam?

A: Please read carefully the instructions on how to correctly fill out the Detailed Reclaim Form. Not providing us with the evidence of the fraudulent activity, can cause that Investigation Partners may not be willing to engage in your case. Please note that each scam/hack should be raised as a separate request. The evidence should be in the following format: .jpg, .png, .pdf, .doc or .xls. Please do not comprise the evidence in the .zip or .rar file. Please do not provide us with your private key and login details.

QUESTION 1. Which cryptocurrency did you lose and how much?

Please specify the amount of lost cryptocurrency. Provide us with the name of the lost cryptocurrency and amount.

Document to be attached: Please provide us with the screenshots of your wallet/exchange account with the details of the fraudulent transaction(s) visible: cryptocurrency address of the scammer; transaction hash; date; amount; type of cryptocurrency. Please do not provide us with the screenshots of blockchain explorers e.g. Etherscan.

QUESTION 2. Could you please provide us with the estimated value of your lost assets in USD ($)?

Please specify the estimated value of your stolen cryptocurrency. To establish its current value you can check the exchange rate on https://coinmarketcap.com/.

QUESTION 3. When did you lose a cryptocurrency?

Please provide us with the exact date(s) when your assets were transferred to the scammer. The dates should be compatible with the dates from the screenshots showing the outgoing transactions from your wallet/exchange account.

If you lost your assets as a consequence of the collapse of some exchange or platform, you can also provide us the dates from the day the entity stopped its operations.

QUESTION 4 Where did you lose your cryptocurrency?

Please provide us with the exact name of the scam platform where you lost your assets. If you have sent your assets to a fake cryptocurrency investor(s), please provide us with the full name(s) of these person(s).

QUESTION 5. How did you lose your cryptocurrency?

Please briefly described how you lost your assets.
E.G., "I sent my assets to platform xxx. Since DD/MM/YYYY I am not able to withdrawal my assets".

QUESTION 6. In which country were you in when you transferred your assets to a scammer/were you hacked/made a transaction in which a loss of cryptocurrency took place?

Please let us know which country you were in when you transferred your assets to a scammer or; you made a transaction in which a loss of cryptocurrency took place.

QUESTION 7. Provide us with wallet addresses from which you lost funds.

If you have sent your assets to a scammer from your wallet, please provide us with the address of the wallet from which the cryptocurrency has been sent.

In case of sending your assets from the exchange, please provide us with the address from which the cryptocurrency has been sent to a scammer. Please note that it is not always the deposit address, where you deposited your funds on the exchange. The exchanges often send the assets from so-called hot wallets. To be sure from which address your assets have been sent to a scammer check the sender address in your transaction history or using transaction hash check it in block explorer (e.g. Etherscan).

QUESTION 8. Could you kindly confirm that you are the owner of the private keys for the addresses specified above? If so, please indicate the name of the wallet application you were using (e.g. Electrum, Exodus, MyEtherWallet, MetaMask).

Please specify if the assets were sent to a scammer from the wallet or cryptocurrency exchange and provide us with the name of the wallet or cryptocurrency exchange that was used for a transfer.

QUESTION 9. Provide us with the scammer's/hacker's wallet addresses

Please provide us with the cryptocurrency address where your assets have been sent e.g. deposit address of scam platform or the address provided to you by a scammer. Please do not provide us with any other addresses.

Document to be attached: The screenshot of a scam platform with the visible deposit address where you have sent your assets; or The email from scam platform confirming the transaction and showing the deposit address or transaction hash; or The screenshot of your transaction history from your scam platform showing the deposit address or transaction hash or The chat/email correspondence with the scammer showing that he/she provided you with the fraudulent address.

QUESTION 10. Please provide us with transactions hashes connected to the case

Please provide us with the transaction hash(es) showing the transfer(s) of your assets to a scammer.

*Transaction hash is a unique attribute used to identify a specific transaction. All blockchain transactions (depositing and withdrawing of funds) have a unique txid that can be found in transaction details. A transaction hash generally looks like a random set of numbers and letters. Transaction hashes are publicly available, and everyone can use them to search for a particular transaction on the block explorer.
For instance, typing a txid in the block explorer (e.g. Blockchain.com) will enable a user to see all the information about the particular transaction: its date, amount, block height, receiver address, etc.
Most trading platforms and cryptocurrency wallets usually have a page presenting the user's transaction history, where transaction hashes can usually be found. If the user cannot find the

transaction hashes in there, he/she should contact the platform/wallet support and ask them for the instructions or providing the needed transaction hashes.

QUESTION 11. Could you please provide us with the deposit/withdrawal bank accounts used by the fraudulent platform/scam service?

If you have sent or received the assets to a scammer via bank account, please provide us with the deposit and/or withdrawal address of the scammer.

Document to be attached: Please provide us with the screenshots of your bank account showing that you have sent and/or you've received the assets from the provided address(es).

QUESTION 12. Have you reported your case to the Law Enforcement (e.g. Police)?

If you have reported your case to the Law Enforcement, please let us know the name of the Law Enforcement you reported your case to, the date and the feedback that you' ve gotten from them.

Document to be attached: Please provide us with the screenshots of the police report related to your case, if available.

QUESTION 13. Have you reported this case to any other organizations, beyond law enforcement?

If you have reported your case to any other organization, please let us know the name of the organization, the feedback you have gotten from them.

Q: What evidence should I provide if I want to report a hack?

A: Please read carefully the instructions on how to correctly fill out the Detailed Reclaim Form. Not providing us with the evidence of the fraudulent activity, can cause that Investigation Partners may not be willing to engage in your case. The evidence should be in the following format: .jpg, .png, .pdf, .doc or .xls. Please do not comprise the evidence in the .zip or .rar file. Please do not provide us with your private key and login details.

QUESTION 1. Which cryptocurrency did you lose and how much?

Please specify the amount of lost cryptocurrency. Provide us with the name of the lost cryptocurrency and amount.

Document to be attached: Please provide us with the screenshots of your wallet/exchange account with the details of the fraudulent transaction(s) visible: cryptocurrency address of the hacker; transaction hash; date; amount; type of cryptocurrency. Please do not provide us with the screenshots of blockchain explorers e.g. Etherscan.

QUESTION 2. Could you please provide us with the estimated value of your lost assets in USD ($)?

Please specify the estimated value of your stolen cryptocurrency. To establish its current value you can check the exchange rate on https://coinmarketcap.com/.

QUESTION 3. When did you lose a cryptocurrency?

Please provide us with the exact date(s) when your assets were hacked.

QUESTION 4. Where did you lose your cryptocurrency?

Please provide us with the exact name of the wallet or the cryptocurrency exchange from which your assets were hacked.

QUESTION 5. How did you lose your cryptocurrency?

Please briefly described how you lost your assets.
E.g. "I've noticed that my crypto was transferred to the unknown wallet on DD/MM/YYYY".

In case of the hack, please provide us with the supporting evidence confirming that your account was hacked.

- If you perform an anti-virus scan on the device connected to the wallet/account, please provide us with the screenshot of the report.
- Please provide us with all emails you received on the day of the hack related to your 2FA; your password change; different IP logs or information that the telephone number which is used to authorize your withdrawals has been changed - If available.
- if you check that your login credentials were hacked (e.g. using the website https://haveibeenpwned.com/), please send us the screenshot of the check results.
- If you lately updated your wallet software or you downloaded some wallet updates, please provide us with the screenshot of the history of your website browser confirming this fact (the screenshot should contain the visible date and name of the website from which the software/update was downloaded).

QUESTION 6. In which country were you in when you transferred your assets to a scammer/were you hacked/made a transaction in which a loss of cryptocurrency took place?

Please let us know which country you were in when your wallet/exchange account was hacked.

QUESTION 7. Provide us with wallet addresses from which you lost funds.

Please provide us with the address of the wallet from which the cryptocurrency has been stolen.

In case of the hack of the exchange account, please provide us with the address from which the cryptocurrency has been hacked. Please note that it is not always the deposit address, where you deposited your funds on the exchange. The exchanges often send the assets from so-called hot wallets. To be sure from which address your assets have been sent to a scammer check the sender address in your transaction history or using transaction hash check it in block explorer (e.g. Etherscan).

QUESTION 8. Could you kindly confirm that you are the owner of the private keys for the addresses specified above? If so, please indicate the name of the wallet application you were using (e.g. Electrum, Exodus, MyEtherWallet, MetaMask).

Please specify if the assets were stolen from the wallet or cryptocurrency exchange and provide us with the name of the wallet or cryptocurrency exchange that was used for a transfer.

Please let us know if you store your SEED/passwords on any electronic device in any form (encrypted or unencrypted). Did you connect the device to the internet/another device connected to the internet? If yes, please describe how you stored this information in detail.

QUESTION 9. Provide us with the scammer's/hacker's wallet address(es)

Please provide us with the cryptocurrency address(es) where your assets have been sent. Please do not provide us with addresses that are not related to your case.

QUESTION 10. Please provide us with transactions hashes connected to the case

Please provide us with the transaction hash(es) showing the transfer(s) of your assets to a hacker.

*Transaction hash is a unique attribute used to identify a specific transaction. All blockchain transactions (depositing and withdrawing of funds) have a unique txid that can be found in transaction details. A transaction hash generally looks like a random set of numbers and letters. Transaction hashes are publicly available, and everyone can use them to search for a particular transaction on the block explorer.
For instance, typing a txid in the block explorer (e.g. Blockchain.com) will enable a user to see all the information about the particular transaction: its date, amount, block height, receiver address, etc.
Most trading platforms and cryptocurrency wallets usually have a page presenting the user's transaction history, where transaction hashes can usually be found. If the user cannot find the transaction hashes in there, he/she should contact the platform/wallet support and ask them for the instructions or providing the needed transaction hashes.

QUESTION 11. Could you please provide us with the deposit/withdrawal bank accounts used by the fraudulent platform/scam service?

The question may be not applicable to cryptocurrency accounts hacks.

QUESTION 12. Have you reported your case to Law Enforcement (e.g. Police)?

If you have reported your case to the Law Enforcement, please let us know the name of the Law Enforcement you reported your case to, the date, and the feedback that you've gotten from them.

Document to be attached: Please provide us with the screenshots of the police report related to your case, if available.

QUESTION 13. Have you reported this case to any other organizations, beyond law enforcement?

If you have reported your case to any other organization, please let us know the name of the organization, the feedback you have gotten from them.

Document to be attached: If possible, please provide us with the screenshots of your email correspondence/chat with your wallet/the exchange support related to your case.

Q: What evidence should I provide if I want to report a phishing scam?

A: Please read carefully the instructions on how to correctly fill out the Detailed Reclaim Form. Not providing us with the evidence of the fraudulent activity, can cause that Investigation Partners may not be willing to engage in your case. The evidence should be in the following format: .jpg, .png, .pdf, .doc or .xls. Please do not comprise the evidence in the .zip or .rar file. Please do not provide us with your private key and login details.

QUESTION 1. Which cryptocurrency did you lose and how much?

Please specify the amount of lost cryptocurrency. Provide us with the name of the lost cryptocurrency and amount.

Document to be attached: Please provide us with the screenshots of your wallet/exchange account with the details of the fraudulent transaction(s) visible: cryptocurrency address of the scammer; transaction hash; date; amount; type of cryptocurrency. Please do not provide us with the screenshots of blockchain explorers e.g. Etherscan.

QUESTION 2. Could you please provide us with the estimated value of your lost assets in USD ($)?

Please specify the estimated value of your stolen cryptocurrency. To establish its current value you can check the exchange rate on https://coinmarketcap.com/.

QUESTION 3. When did you lose a cryptocurrency?

Please provide us with the exact date(s) when your assets were transferred to the scammer. The dates should be compatible with the dates from the screenshots showing the outgoing transactions from your wallet/exchange account.

QUESTION 4. Where did you lose your cryptocurrency?

Please provide us with the exact name of the scam where you lost your assets e.g. Fake Ripple Website; Fake Electrum Wallet.

QUESTION 5. How did you lose your cryptocurrency?

Please briefly described how you lost your assets.
E.G., "I've received an email from someone that falsely claimed is from Coinbase support. I've clicked on the provided link and I inserted my login credentials. Two days later I've noticed that my assets were gone" or "I've downloaded fake MetaMask extension. I connected my wallet to this extension and my assets disappeared".

In case of a phishing scam, please provide us with supporting evidence confirming the event.

- The screenshots of emails received from the scammers.
- The screenshots of your browser history confirming that you have downloaded a fake software (the screenshot should contain the visible date and name of the website from which the software was downloaded).

QUESTION 6. In which country were you in when you transferred your assets to a scammer/were you hacked/made a transaction in which a loss of cryptocurrency took place?

Please let us know which country you were in when your assets were transferred to a scammer or; you made a transaction in which a loss of cryptocurrency took place.

QUESTION 7. Provide us with wallet addresses from which you lost funds.

Please provide us with the address of the wallet from which the cryptocurrency has been sent.

In case of sending your assets from the exchange, please provide us with the address from which the cryptocurrency has been sent to a scammer. Please note that it is not always the deposit address, where you deposited your funds on the exchange. The exchanges often send the assets from so-called hot wallets. To be sure from which address your assets have been sent to a scammer check the sender address in your transaction history or using transaction hash check it in block explorer (e.g. Etherscan).

QUESTION 8. Could you kindly confirm that you are the owner of the private keys for the addresses specified above? If so, please indicate the name of the wallet application you were using (e.g. Electrum, Exodus, MyEtherWallet, MetaMask).

Please specify if the assets were sent to a scammer from the wallet or cryptocurrency exchange and provide us with the name of the wallet or cryptocurrency exchange that was used for a transfer.

QUESTION 9. Provide us with the scammer's/hacker's wallet addresses

Please provide us with the cryptocurrency address where your assets have been sent. Please do not provide us with any other addresses.

Document to be attached: If the scammer provided you with the fraudulent wallet address where your assets have been sent, please attach the screenshot confirming this fact.

QUESTION 10. Please provide us with transactions hashes connected to the case

Please provide us with the transaction hash(es) showing the transfer(s) of your assets to a scammer.

*Transaction hash is a unique attribute used to identify a specific transaction. All blockchain transactions (depositing and withdrawing of funds) have a unique txid that can be found in transaction details. A transaction hash generally looks like a random set of numbers and letters. Transaction hashes are publicly available, and everyone can use them to search for a particular transaction on the block explorer.
For instance, typing a txid in the block explorer (e.g. Blockchain.com) will enable a user to see all the information about the particular transaction: its date, amount, block height, receiver address, etc.
Most trading platforms and cryptocurrency wallets usually have a page presenting the user's transaction history, where transaction hashes can usually be found. If the user cannot find the transaction hashes in there, he/she should contact the platform/wallet support and ask them for the instructions or providing the needed transaction hashes.

QUESTION 11. Could you please provide us with the deposit/withdrawal bank accounts used by the fraudulent platform/scam service?

If you have sent or received the assets to a scammer via bank account, please provide us with the deposit and/or withdrawal address of the scammer.

Document to be attached: Please provide us with the screenshots of your bank account showing that you have sent and/or you've received the assets from the provided address(es).

QUESTION 12. Have you reported your case to Law Enforcement (e.g. Police)?

If you have reported your case to the Law Enforcement, please let us know the name of the Law Enforcement you reported your case to, the date, and the feedback that you've gotten from them.

Document to be attached: Please provide us with the screenshots of the police report related to your case, if available.

QUESTION 13. Have you reported this case to any other organizations, beyond law enforcement?

If you have reported your case to any other organization, please let us know the name of the organization, the feedback you have gotten from them.

Q: What evidence should I provide if I want to report a fake giveaway/airdrop scam?

A: Please read carefully the instructions on how to correctly fill out the Detailed Reclaim Form. Not providing us with the evidence of the fraudulent activity, can cause that Investigation Partners may not be willing to engage in your case. The evidence should be in the following format: .jpg, .png, .pdf, .doc or .xls. Please do not comprise the evidence in the .zip or .rar file. Please do not provide us with your private key and login details.

QUESTION 1. Which cryptocurrency did you lose and how much?

Please specify the amount of lost cryptocurrency. Provide us with the name of the lost cryptocurrency and amount.

Document to be attached: Please provide us with the screenshots of your wallet/exchange account with the details of the fraudulent transaction(s) visible: cryptocurrency address of the scammer; transaction hash; date; amount; type of cryptocurrency. Please do not provide us with the screenshots of blockchain explorers e.g. Etherscan.

QUESTION 2. Could you please provide us with the estimated value of your lost assets in USD ($)?

Please specify the estimated value of your stolen cryptocurrency. To establish its current value you can check the exchange rate on https://coinmarketcap.com/.

QUESTION 3. When did you lose a cryptocurrency?

Please provide us with the exact date(s) when your assets were transferred to the scammer. The dates should be compatible with the dates from the screenshots showing the outgoing transactions from your wallet/exchange account.

QUESTION 4 Where did you lose your cryptocurrency?

Please provide us with the exact name of the scam where you lost your assets e.g. Fake Ripple Airdrop on YouTube; Fake BTC Giveaway on Twitter. Please add the exact address of the fraudulent website or YouTube video, Twitter post if possible.

QUESTION 5. How did you lose your cryptocurrency?

Please briefly described how you lost your assets.
E.G., "I've watched YouTube video where Mr.XX YY promised to double my BTC. Further, I went to the provided website www.<name of the webiste>.com and I sent my BTC on the address visible on the website".

QUESTION 6. In which country were you in when you transferred your assets to a scammer/were you hacked/made a transaction in which a loss of cryptocurrency took place?

Please let us know which country you were in when your assets were transferred to a scammer or; you made a transaction in which a loss of cryptocurrency took place.

QUESTION 7. Provide us with wallet addresses from which you lost funds.

Please provide us with the address of the wallet from which the cryptocurrency has been sent.

In case of sending your assets from the exchange, please provide us with the address from which the cryptocurrency has been sent to a scammer. Please note that it is not always the deposit address, where you deposited your funds on the exchange. The exchanges often send the assets from so-called hot wallets. To be sure from which address your assets have been sent to a scammer check the sender address in your transaction history or using transaction hash check it in block explorer (e.g. Etherscan).

QUESTION 8. Could you kindly confirm that you are the owner of the private keys for the addresses specified above? If so, please indicate the name of the wallet application you were using (e.g. Electrum, Exodus, MyEtherWallet, MetaMask).

Please specify if the assets were sent to a scammer from the wallet or cryptocurrency exchange and provide us with the name of the wallet or cryptocurrency exchange that was used for a transfer.

QUESTION 9. Provide us with the scammer's/hacker's wallet addresses

Please provide us with the cryptocurrency address where your assets have been sent. Please do not provide us with any other addresses.

Document to be attached: Please attach a screenshot showing the mentioned website or YouTube video with the fraudulent address visible.

QUESTION 10. Please provide us with transactions hashes connected to the case

Please provide us with the transaction hash(es) showing the transfer(s) of your assets to a scammer.

*Transaction hash is a unique attribute used to identify a specific transaction. All blockchain transactions (depositing and withdrawing of funds) have a unique txid that can be found in

transaction details. A transaction hash generally looks like a random set of numbers and letters. Transaction hashes are publicly available, and everyone can use them to search for a particular transaction on the block explorer.
For instance, typing a txid in the block explorer (e.g. Blockchain.com) will enable a user to see all the information about the particular transaction: its date, amount, block height, receiver address, etc.
Most trading platforms and cryptocurrency wallets usually have a page presenting the user's transaction history, where transaction hashes can usually be found. If the user cannot find the transaction hashes in there, he/she should contact the platform/wallet support and ask them for the instructions or providing the needed transaction hashes.

QUESTION 11. Could you please provide us with the deposit/withdrawal bank accounts used by the fraudulent platform/scam service?

If you have sent or received the assets to a scammer via bank account, please provide us with the deposit and/or withdrawal address of the scammer.

Document to be attached: Please provide us with the screenshots of your bank account showing that you have sent and/or you've received the assets from the provided address(es).

QUESTION 12. Have you reported your case to Law Enforcement (e.g. Police)?

If you have reported your case to the Law Enforcement, please let us know the name of the Law Enforcement you reported your case to, the date, and the feedback that you've gotten from them.

Document to be attached: Please provide us with the screenshots of the police report related to your case, if available.

QUESTION 13. Have you reported this case to any other organizations, beyond law enforcement?

If you have reported your case to any other organization, please let us know the name of the organization, the feedback you have gotten from them.