ComplyFirst

EXAMPLE PRIVACY FEATURE ENHANCED DUE DILIGENCE QUESTIONNAIRE

Cryptocurrency privacy features may be added on top of any cryptocurrency, including output-based and account-based cryptocurrencies. In cases where a relatively uncommon privacy feature is detected, you can adapt this questionnaire to learn more information about the user's transactions. Depending on the responses, you may find it necessary to file a suspicious transaction report with your regulator.

Not all of these questions may be relevant or necessary for your customers and counterparties. You must adapt this questionnaire in a way that is appropriate. This questionnaire may not be appropriate or realistic for users of cryptocurrencies with intrinsic privacy-enhancing properties, for which the use of these privacy-enhancing features may be a less reliable indicator of increased risk. In any case, only use this questionnaire as one possible method among all possible risk-mitigation methods.

The questionnaire begins on the next page. ***Do not send this page to customers.***

ComplyFirst

PRIVACY FEATURE ENHANCED DUE DILIGENCE QUESTIONNAIRE

Our service takes the responsibility of only accepting clean coins that are not related to any illegal or undesired activities seriously. Our compliance monitoring or onboarding process has detected that you may be involved with privacy-enhancing activities such as mixing services, shielded transactions, or other unusual privacy-enhancing behaviors for your cryptocurrency network. As such, we ask that you complete this questionnaire to help us better understand the source of your funds and your motives for using advanced privacy-enhancing services and/or tools. Based on your responses, we may require additional supporting documentation or have follow-up questions.

Onboarded Individual or Entity name:

Account number/identifier (if applicable): **Date:**
Email: **Phone:**
Regulators and/or licenses held:

Privacy-enhancing features/services and wallets used:

If applicable, explain how you acquired these funds and the source of these funds:

If applicable, explain how you spent/used these withdrawn funds:

If you used a privacy-enhancing service or feature, complete the following:

Describe your process of using a privacy-enhancing feature to the best of your ability:

Describe why you are using a privacy-enhancing feature:

What cryptocurrency addresses did you use before/during/after (as applicable) the privacy-enhancing feature?

What cryptocurrency transactions were involved before/during/after (as applicable) the privacy-enhancing feature?

If the privacy-enhancing process was interactive, did you conduct due diligence (eg: collect IDs, physical addresses, etc.) or otherwise know any of the counterparties you interacted with to use this privacy-enhancing feature? If so, provide as much information as possible, including names and wallet addresses:

Do you intend to use these or similar privacy-enhancing features in the future? If so, why?

If you did not directly use a privacy-enhancing feature but suspect you may have sent/received funds related to someone who did, complete the following:

Describe in detail where you received coins from or sent coins to:

Describe why you are receiving or sending cryptocurrency:

Describe if/how you monitor coins for potential undesirable (“tainted”) history:

If you use a payment processor, explain what payment processor you use. Explain the process of receiving coins in detail:

If you offer a product or service, describe what products and services you offer:

Include the following with your response, if applicable:

1. Unredacted copies of your bank statement(s)
2. Receipts for invoices, purchases, and/or sales (as applicable) of cryptocurrencies with undesirable histories
3. Other statements showing significant assets of you or your entity
4. Screenshot/proof of transactions and wallets involved with the privacy-enhancing service or tool, or screenshots related to the affected wallets
5. AML/KYC policies and procedures
6. Proof of using chain analysis software
7. Proof of involved wallets controlled by you or your entity
8. List of remediative actions taken against your customer/counterparty who associated you with these undesired activities