Merchant Guidance

Introduction

Blockchain technologies radically differ from traditional fiat currency transactions. That is why monitoring techniques have to be updated in accordance with the opportunities provided by blockchain improvements. At Cryptopay we believe that illicit activity in cryptocurrency can and must be disrupted to stop criminals from harming our customers' reputation and business. To solve this problem, Cryptopay has established an ongoing cryptocurrency monitoring based on the regulator recommendations using a risk-based approach. We achieved this goal by implementing modern monitoring tools analysing blockchain connections and developing an appropriate risk assessment system.

What is BitScore?

Bitscore is an internal blockchain analysis tool, which identifies risk of the cryptocurrency transactions. It identifies the beneficiaries of a cryptocurrency transaction and evaluates the risk score. The BitScore uses risk rules to identify any flag the suspicious transaction.

How does it work?

In a traditional fiat world, banks are able to see immediate beneficiaries and originators who exchange transactions with their customers as all the intermediaries are regulated. However, banks have less insight into the flow of funds as they do not know its genuine source and destination.

In the crypto world the situation is reversed, as crypto business lacks information about the identity of the immediate beneficiaries and originators. But due to crypto monitoring technologies, the analysis beyond the immediate transaction with a customer is possible now. Thanks to blockchain nature, we can track all the cryptocurrency transactions step by step «block by block». Hence, blockchain monitoring solutions like those we use at Cryptopay help us understand the genuine source and destination of funds, which allows us subsequent protection of our customers' business by assessing a risk level of transactions.

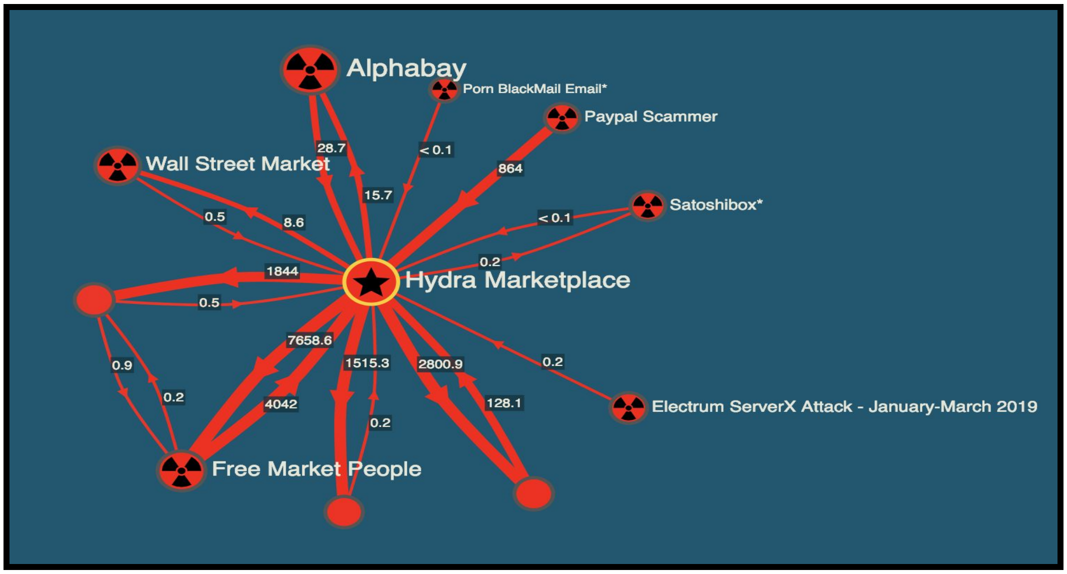
Risk Assessment and Risk Rules

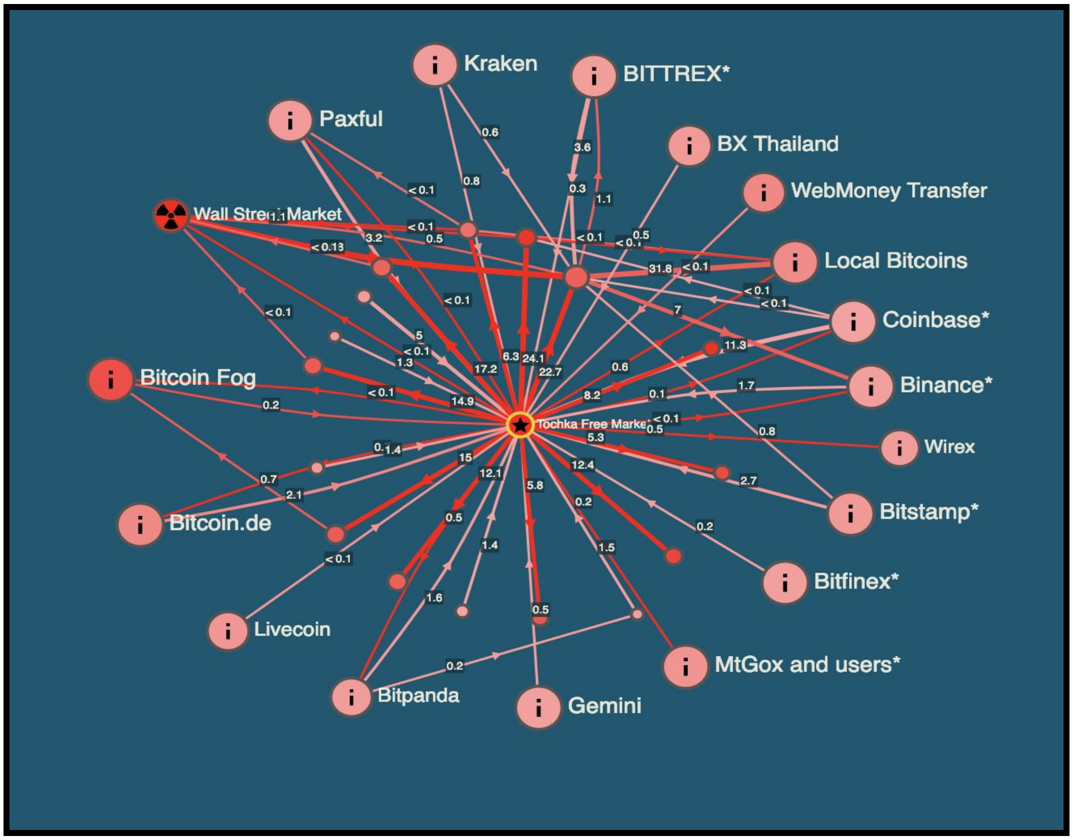
At Cryptopay we review transactions that generate a risk score above a certain threshold regardless of internal rules triggered. A Risk Rule is a group of parameters defined by us in accordance with the regulatory requirements. Cryptopay developed a system of Risk Rules which creates conditions for calculating a risk score for every incoming or outgoing transaction. This system is based on counteracting activities tied with the following categories:

- **Dark markets and criminal organisations**: Child Sexual Abuse Material, Criminal Event, Criminal Organisations, Known Criminal, Terrorist Organisation, Ransomware, Scam, Theft, Malware, Fake ICO, Dark Market - Centralised, Dark Market - Decentralised, Dark Market - Forum, Dark Market - Vendor Shop, Dark Vendor, Dark Service, Investment, Fake ICO
- **Fraudulent resources**: Malware, Ponzi Scheme, Ransomware, Scam, Theft, Phishing
- **Mixers** (Tumblers) and Investments (ex. ICO, Escrow)

What are Darknet resources and why are they dangerous?

A darknet market is a commercial website that operates via illegal sources like Tor or I2P and functions primarily as black markets where drugs, weapons, cyber-arms, stolen credit card details, forged documents and other illicit goods can be exchanged for cryptocurrency payments.





Every transaction, connected to such resources, means that a customer can be aligned with illicit activities. According to the authorities' and regulatory requirements, any connections to such resources must be prevented. Because of the dangerous nature of activities related to darknet resources unexpected harm can be done to business.

What about GDPR?

Due to the GDPR directive some merchants must not share some of the information requested.

However, under the Data Protection Act 2018 (Schedule 2, Part 1 Paragraph 2) an organisation is allowed to disclose personal data to a third party in circumstances where the organisation would otherwise be prevented from doing so by the GDPR, where the disclosure and processing of personal data is for one of the following purposes:

- the prevention or detection of crime,
- the apprehension or prosecution of offenders, or
- the assessment or collection of a tax or duty or an imposition of a similar nature; AND
- where not disclosing information would prejudice any of the above three purposes

NOTE:

The request does not create any obligation to disclose information. It merely confirms that the purpose for which information is required does not contravene the terms of the Data Protection Act 2018. For more details on Schedule 2, Part 1 Paragraph 2 please see Appendix 1.

Appendix 1

Data Protection Act 2018- (Schedule 2- Exemptions Etc. from the GDPR- Part 1 Paragraph 2)

Crime and taxation: general

2 (1) The listed GDPR provisions and Article 34(1) and (4) of the GDPR (communication of personal data breach to the data subject) do not apply to personal data processed for any of the

following purposes-

(a) the prevention or detection of crime,

(b) the apprehension or prosecution of offenders, or

(c) the assessment or collection of a tax or duty or an imposition of a similar nature,

to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) to (c).

(2) Sub-paragraph (3) applies where-

(a) personal data is processed by a person (“Controller 1”) for any of the purposes mentioned in sub-paragraph (1)(a) to (c), and

(b) another person (“Controller 2") obtains the data from Controller 1 for the purpose of discharging statutory functions and processes it for the purpose of discharging statutory functions.

(3) Controller 2 is exempt from the obligations in the following provisions of the GDPR-

(a) Article 13(1) to (3) (personal data collected from data subject: information to be provided),

(b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided),

(c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers), and

(d) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in paragraphs (a) to (c),

to the same extent that Controller 1 is exempt from those obligations by virtue of sub-paragraph (1).

High-Risk transactions

In the process of transaction analysis, a risk level is assigned for each transaction. There are 3 risk levels in Cryptopay practice:

- Low-Risk: transactions are not risky
- Medium-Risk: transactions might be connected to darknet resources indirectly
- High-Risk: transactions are related to darknet resources

After risk analysis, High-Risk transactions get to the next step when the Transaction Monitoring team investigates every transaction in order to exclude the possibility of a false-positive match. If a connection with darknet resources is confirmed, the Transaction Monitoring team notifies Cryptopay customers about them and gives recommendations in order to avoid potential harm.

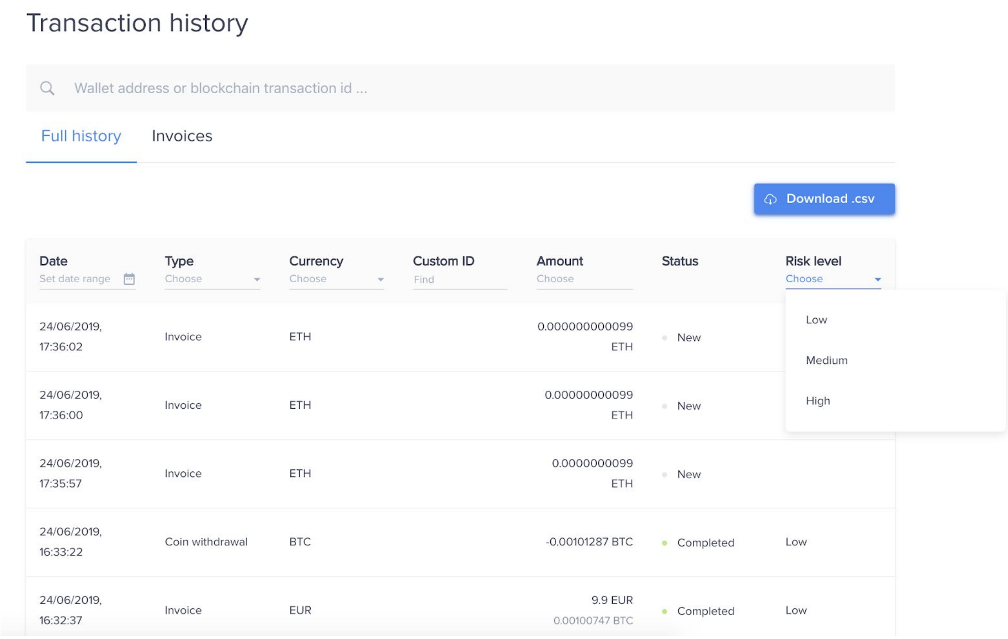
According to our internal transaction policies and the regulatory requirements, Cryptopay is obliged to conduct due diligence to clients connected with High-Risk transactions. This way, if High-Risk transactions arise additional suspicions, the Transaction Monitoring team may require further explanations and extra information about them. Extra details include the following categories:

- Identification of a person who made a high-risk transaction
- Customer First/Last name
- Email address/Phone number
- Bank account details
- Details of the customer KYC records
- Current Address (Country, City, Address, Zip)

Due to the importance of issues related to the implementation of anti-money laundering standards, Cryptopay expects merchants to provide the requested information within 10 days.

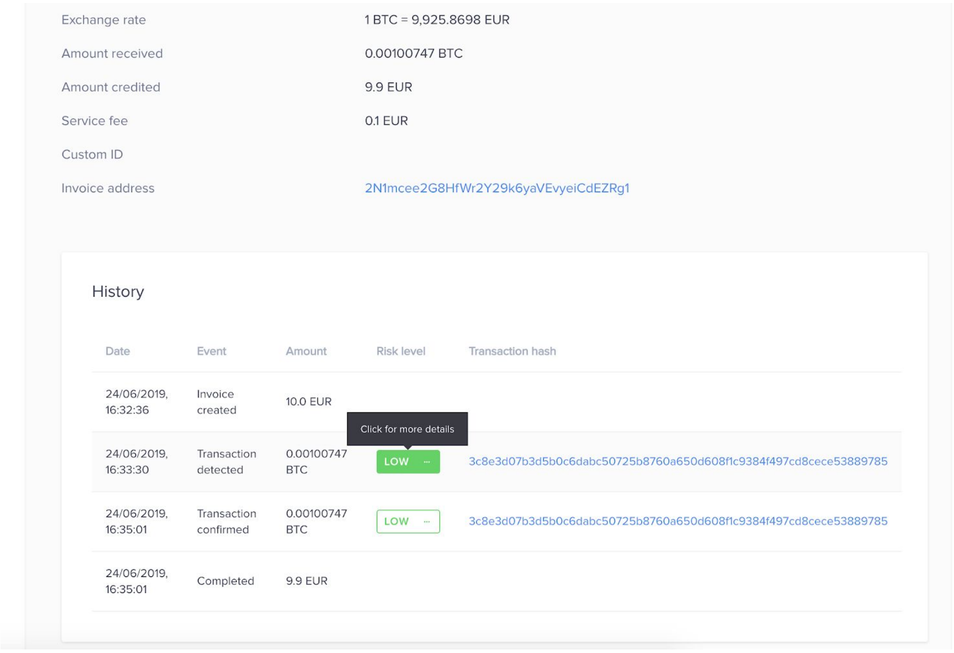
How to detect High-Risk transactions yourself?

Merchants are able to trace High-Risk transactions themselves. There is a Transaction History page in your business account with an option to filter transactions choosing risk level. When you open transaction details you are also able to check risk information related to a particular transaction.



Transaction history

Date	Type	Currency	Custom ID	Amount	Status	Risk level
24/06/2019, 17:36:02	Invoice	ETH		0.000000000099 ETH	New	
24/06/2019, 17:36:00	Invoice	ETH		0.00000000099 ETH	New	
24/06/2019, 17:35:57	Invoice	ETH		0.0000000099 ETH	New	
24/06/2019, 16:33:22	Coin withdrawal	BTC		-0.00101287 BTC	Completed	Low
24/06/2019, 16:32:37	Invoice	EUR		9.9 EUR 0.00100747 BTC	Completed	Low

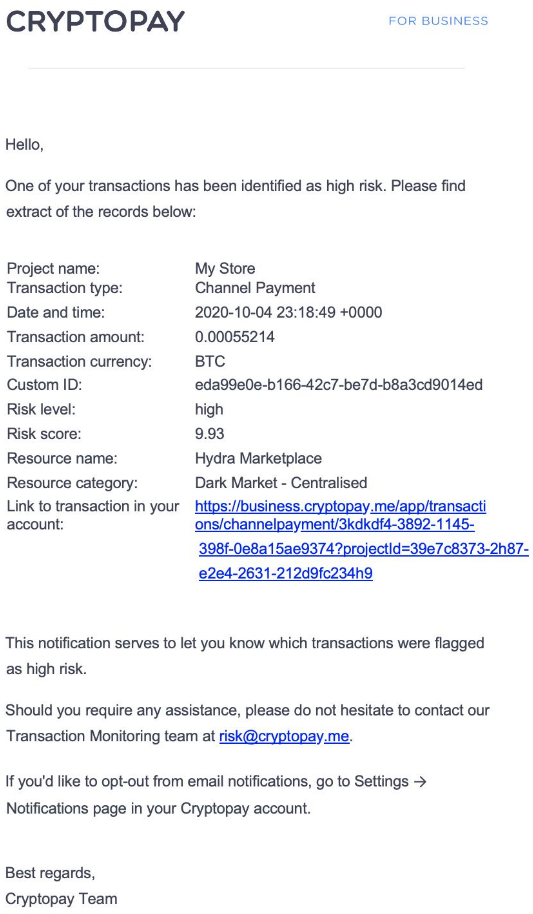


Exchange rate	1 BTC = 9,925.8698 EUR
Amount received	0.00100747 BTC
Amount credited	9.9 EUR
Service fee	0.1 EUR
Custom ID	
Invoice address	2N1mcee2G8HfWr2Y29k6yaVEvyeiCdEZRg1

History

Date	Event	Amount	Risk level	Transaction hash
24/06/2019, 16:32:36	Invoice created	10.0 EUR		
24/06/2019, 16:33:30	Transaction detected	0.00100747 BTC	LOW	3c8e3d07b3d5b0c6dabc50725b8760a650d608f1c9384f497cd8cece53889785
24/06/2019, 16:35:01	Transaction confirmed	0.00100747 BTC	LOW	3c8e3d07b3d5b0c6dabc50725b8760a650d608f1c9384f497cd8cece53889785
24/06/2019, 16:35:01	Completed	9.9 EUR		

Despite the fact that TM team notifies Cryptopay clients about High-Risk transactions, merchants are able to receive such notifications automatically which allows early action to prevent recurrence of High-Risk transactions and reduce the risks related to money laundering during company’s business activity. That is why Cryptopay highly recommends subscribing to instant email notifications in Settings > Notifications.



Hello,

One of your transactions has been identified as high risk. Please find extract of the records below:

Project name:	My Store
Transaction type:	Channel Payment
Date and time:	2020-10-04 23:18:49 +0000
Transaction amount:	0.00055214
Transaction currency:	BTC
Custom ID:	eda99e0e-b166-42c7-be7d-b8a3cd9014ed
Risk level:	high
Risk score:	9.93
Resource name:	Hydra Marketplace
Resource category:	Dark Market - Centralised
Link to transaction in your account:	https://business.cryptopay.me/app/transactions/channelpayment/3kdkdf4-3892-1145-398f-0e8a15ae9374?projectId=39e7c8373-2h87-e2e4-2631-212d9fc234h9

This notification serves to let you know which transactions were flagged as high risk.

Should you require any assistance, please do not hesitate to contact our Transaction Monitoring team at risk@cryptopay.me.

If you'd like to opt-out from email notifications, go to Settings → Notifications page in your Cryptopay account.

Best regards,
Cryptopay Team

What De-Risk actions to choose?

In order to decrease the risk level when High-Risk transactions are detected it is highly recommended to apply at least one of the following actions:

- Refreshing CDD
- Requesting "Source of Funds" Declaration
- Applying account limitations
- Terminating business relationships with a client

One should also know that merchants are required to take appropriate actions to comply with local laws and their own AML/KYC policy, which should be aimed at minimising the risks of money laundering and other criminal activity that may occur while providing services to customers. In this case Cryptopay expects cooperation with its clients in order to continue doing business in compliance with AML standards.

What is CDD?

Customer Due Diligence or CDD, is the process where relevant information about the client is collected and evaluated for any potential risk for the organization or money laundering/terrorist financing activities. This information should be confirmed with evidence like proofs of identity (national identity cards, passports, driving licences etc) or proofs of address (bank statements, residence certificates, utility bills etc). Some cases require implementing additional measures as a confirmation of the source of funds.

Source of funds check is a way of asking clients to send some form of proof, to show that funds come from a legitimate source - either salary, or business profit, or a bank loan, etc. All the explanations should be confirmed by financial documents.

In practice, Cryptopay expects the merchants to be able to provide documents which identify the person who committed a High-Risk transaction like a proof of ID and a proof of address. This information helps to protect customers' business.

Contacts

If you are not sure what to do, by defining a high-risk transaction, you can contact with Transaction Monitoring team via risk@cryptopay.me or write to the Support Team via support@cryptopay.me and they will escalate your case to the relevant team.