

Crypto Risk Management Policy

1. We use the Chainalysis Risk Tool as the main tool for mitigating funds risk.
2. All of the payments in and out are monitored with the tool.
3. Based on proximity and value we have an automated set of rules that are triggered upon receiving or sending request:

Severity	Category	Direction	Exposure Type	USD Range	Percentage of transfer range
MEDIUM	ransomware	SENT	DIRECT	[500,)	[0,100]
MEDIUM	ransomware	RECEIVED	DIRECT	[10,100)	[0,100]
HIGH	ransomware	RECEIVED	DIRECT	[100,)	[0,100]
MEDIUM	mixing	RECEIVED	DIRECT	[500,)	[0,100]
MEDIUM	mixing	SENT	DIRECT	[500,)	[0,100]
SEVERE	sanctioned entity	RECEIVED	DIRECT	(0,)	[0,100]
SEVERE	sanctioned entity	SENT	DIRECT	(0,)	[0,100]
SEVERE	child abuse material	RECEIVED	DIRECT	(0,)	[0,100]
SEVERE	child abuse material	SENT	DIRECT	(0,)	[0,100]
MEDIUM	p2p exchange	RECEIVED	DIRECT	[500,)	[0,100]
MEDIUM	p2p exchange	SENT	DIRECT	[500,)	[0,100]
SEVERE	terrorist financing	RECEIVED	DIRECT	(0,)	[0,100]
SEVERE	terrorist financing	SENT	DIRECT	(0,)	[0,100]
MEDIUM	darknet market	RECEIVED	DIRECT	[10,100)	[0,100]
MEDIUM	darknet market	SENT	DIRECT	[10,100)	[0,100]
HIGH	darknet market	RECEIVED	DIRECT	[100,)	[0,100]
HIGH	darknet market	SENT	DIRECT	[100,)	[0,100]
MEDIUM	scam	SENT	DIRECT	[500,)	[0,100]
MEDIUM	scam	RECEIVED	DIRECT	[10,100)	[0,100]
HIGH	scam	RECEIVED	DIRECT	[100,)	[0,100]
SEVERE	child abuse material	RECEIVED	INDIRECT	(0,)	[30,100]
SEVERE	child abuse material	SENT	INDIRECT	(0,)	[0,100]
HIGH	stolen funds	RECEIVED	DIRECT	(0,)	[0,100]
MEDIUM	stolen funds	SENT	DIRECT	[500,)	[0,100]
LOW		RECEIVED	DIRECT	[1000000,)	[0,100]
LOW		SENT	DIRECT	[1000000,)	[0,100]
MEDIUM	no kyc exchange	RECEIVED	DIRECT	[500,)	[0,100]

MEDIUM	no kyc exchange	SENT	DIRECT	[500,)	[0,100]
HIGH	custom address	SENT	DIRECT	[5,)	[0,100]
HIGH	atm	SENT	DIRECT	[1000,)	[0,100]
HIGH	atm	RECEIVED	DIRECT	[1000,)	[0,100]
HIGH	sanctioned jurisdiction	SENT	DIRECT	[5,)	[0,100]
HIGH	sanctioned jurisdiction	RECEIVED	DIRECT	[5,)	[0,100]
MEDIUM	sanctioned jurisdiction	SENT	DIRECT	(0,5)	[0,100]
MEDIUM	sanctioned jurisdiction	RECEIVED	DIRECT	(0,5)	[0,100]
MEDIUM	protocol privacy	RECEIVED	DIRECT	[500,)	[0,100]
MEDIUM	protocol privacy	SENT	DIRECT	[500,)	[0,100]
MEDIUM	fraud shop	SENT	DIRECT	[10,100)	[0,100]
MEDIUM	illicit actor-org	SENT	DIRECT	[10,100)	[0,100]
MEDIUM	infrastructure as a service	SENT	DIRECT	[500,)	[0,100]
HIGH	fraud shop	SENT	DIRECT	[100,)	[0,100]
HIGH	illicit actor-org	SENT	DIRECT	[100,)	[0,100]
MEDIUM	fraud shop	RECEIVED	DIRECT	[10,100)	[0,100]
MEDIUM	illicit actor-org	RECEIVED	DIRECT	[10,100)	[0,100]
MEDIUM	infrastructure as a service	RECEIVED	DIRECT	[500,)	[0,100]
HIGH	fraud shop	RECEIVED	DIRECT	[100,)	[0,100]
HIGH	illicit actor-org	RECEIVED	DIRECT	[100,)	[0,100]
SEVERE	special measures	SENT	DIRECT	(0,)	[0,100]
SEVERE	special measures	RECEIVED	DIRECT	(0,)	[0,100]
HIGH	online pharmacy	RECEIVED	DIRECT	[100,)	[0,100]
HIGH	online pharmacy	SENT	DIRECT	[100,)	[0,100]
MEDIUM	online pharmacy	RECEIVED	DIRECT	[10,100)	[0,100]
MEDIUM	online pharmacy	SENT	DIRECT	[10,100)	[0,100]
HIGH	malware	RECEIVED	DIRECT	[100,)	[0,100]
HIGH	malware	SENT	DIRECT	[100,)	[0,100]
MEDIUM	malware	RECEIVED	DIRECT	[10,100)	[0,100]
MEDIUM	malware	SENT	DIRECT	[10,100)	[0,100]

MEDIUM	darknet market	SENT	INDIRECT	[100,)	[20,100]
--------	----------------	------	----------	--------	----------

4. If the direct funding (deposit) from a suspicious source happens the first time our Fraud and Payments Team will make relevant account tagging and comments.
5. If the direct funding (deposit) from a suspicious source occurs more than ones in the same fashion our Fraud and Payments Team will make a relevant internal STR escalation.
6. If direct funding of a payout wallet is requested (withdrawal) our tools allow monitoring making decisions prior to sending the money. In such a case, we will proceed to internal STR.
 - 6.1. Depending on the category, percentage of direct funding to the exposed wallet and account history, we may decide to either send the money or withhold it for FIU STR escalation.
 - 6.2. Chainalysis OSINT information can be very detailed and descriptive. Therefore it is not possible to anticipate all variables comprising the decision. As such the decision remains an arbitrary decision of the Compliance Officer.
7. In all cases we apply risk based approach:

	Negligible	Minor	Moderate	Significant	Severe
Very likely	User making deposits with Direct Exposure from another Gambling Company.	Users making multiple registrations abusing reward schemes.	Users with Indirect Exposure deposits with High Risk Category via an exchange of high KYC standards.	Less than a 100 USD deposit from High Risk Category and Direct Exposure without a possibility to "chip dump" or "opposite bet" i.e. without an option to launder the funds.	Less than a 100 USD deposit from High Risk Category and Direct Exposure who plays live games of 2 outcomes.
Likely	Users with Indirect Exposure deposits with Medium Risk exposure via an exchange of low KYC standards.	Users making multiple registrations.	Users making less than 100 USD deposit with Direct Exposure to Darknet Markets and spending it all without ability to launder it and without relationship to other accounts through behaviour and source of funds.	Repetitive funding of an account with Direct Exposure (deposits) from High Severity Category of total value of less than 500 without a possibility to "chip dump" or "opposite bet" i.e. without an option to launder the funds.	Less than a 1000 USD deposit from High Risk Category and Direct Exposure who plays live games of 2 outcomes.
Possible	Users with Indirect Exposure deposits with High Risk exposure via an exchange of low KYC standards.	Users with Indirect Exposure deposits with High Risk exposure via an exchange of low KYC standards.	Over 1000 USD High Risk Category Direct Exposure deposit without a possibility to "chip dump" or "opposite bet" i.e. without an option to launder the funds.	User disguising the Exposure through a set of non-custodial wallets.	
Unlikely	Less than a 100 USD deposit from High Risk Category and Direct Exposure and consequent withdrawal of the said funds.	Less than a 500 USD deposit from High Risk Category and Direct Exposure and consequent withdrawal of the said funds.	Over 20000 USD High Risk Category Direct Exposure deposit without a possibility to "chip dump" or "opposite bet" i.e. without an option to launder the funds.	1. Phishing of funded user's accounts. 2. Over 20000 USD High Risk Category Direct Exposure funding.	1. Payout to a fraudster's wallet based on a phishing attack. 2. Payout to a wallet of a High Risk Category; payout to a wallet of funds coming from deposit of High Risk Category and Direct Exposure.
Very Unlikely	User making a 1000000 USD deposit with Indirect Exposure to High Risk Category via Crypto Exchange of high KYC standards.	User making a 1000000 USD deposit with Indirect Exposure to High Risk Category via Crypto Exchange of low KYC standards.		User making a 1000000 USD deposit with non-custodial wallet with Direct Exposure to Darknet or CAM Category.	Hacking of our wallets with Coinspaid.