REV 1.1 to 1.4 7-29-25 1032, REV 2.1 8-2-2025

---

***********IMPORTANT************

**INVESTIGATION INVOLVING ANOTHER ENTITY (ECI DEVELOPPMENT) SURROUNDING OSC SECURITIES FRAUD IS UNDER INVESTIGATION WITH ME INVOLVED. THIS IS HOW I HAVE BEEN ABLE TO TRACK, TRACE AND REPORT THIS INFORMATION SO QUICKLY. I NOW HAVE A BACKGROUND IN UNDERSTANDING HOW AML AND KYC WORKS, AS WELL AS THE RELEVANT CRIMINAL CODES BROKEN.**

**THIS MAY BE THIS IS LINKED TO POTENTIAL GANG STALKING AS I UPSET SEVERAL HIGH LEVEL "AUTHORITIES" BY REVEALING WHAT I HAD UNCOVERED AFTER YEARS OF MY INVESTIGATION WITH ECI DEVELOPMENT (SINCE 2021). FULL DISCLOSURE, THIS MAY BE LINKED TO RCMP CASE NUMBER 2025-55862, AND OSC WHISTLEBLOWER CASE REF NUMBER 467-540**

---

COMPLAINT

---

**POTENTIAL FRAUD / COLLUSION / THEFT / TARGETING / RACKETEERING**

---

**MEXC** AND **FORIS DAX CAN ULC** IN POTENTIAL COLLUSION OF FRAUD, THEFT, IMPLICIT CUSTOMER TARGETING, RACKETEERING, POZI SCHEME

I am fully aware of implications of false reporting. Below is a full report of what I have uncovered to be collusion of MEXC (possibly other exchanges), and FORIS DAX CAN ULC. *NOTE – I will be moving my crypto OFF Crypto.com to an official Canadian Bank slowly to avoid them blocking any further funds as I see the entire crypto market as now being involved in dubious activities.*

Below complaint is for a transfer of funds from MEXC to FORIS DAX CAN ULC (Crypto.com)

This complaint outlines collusion practices of MEXC and FORIS DAX CAN ULC for intentional theft of crypto currencies on a potentially mass scale and market manipulation.

---

**Complaint about the following OSC registered entity**

---

Registration for Crypto.com (FORIS DAX CAN ULC operating under Crypto.com registered in the OSC) , Address FORIS DAX CAN ULC #1700, 421 7th Avenue SW, Calgary, Alberta, T2P4K9

→ https://drive.google.com/file/d/1SW33WAc_I8ZlO43vpZ0LmQ1dtbw-zCF7/view?usp=drive_link
→ https://drive.google.com/file/d/1Z-kt8TJazFm722bwXTKci1bWlar_-dcj/view?usp=drive_link

FORIS DAX CAN ULC REGISTRANT 1 – Becky Cantanese, 110N College Ave, Suite 500 Tyler TX, 75702, PHONE (305)539-0413
→ https://drive.google.com/file/d/1f2L3k1oDC0yL572fxdpDhgXuuCvcjzML/view?usp=drive_link
FORIS DAX CAN ULC REGISTRANT 2 – James Grabow, 110N College Ave, Suite 500 Tyler TX, 75702, PHONE (305)539-0413
→ https://drive.google.com/file/d/1cXlZTc_y2PPEIXW8GuR_ZbZUFppin6cz/view?usp=drive_link

FORIS DAC CAN ULC REGISTERED WITH THE OSC
→ https://drive.google.com/file/d/1HAExIJRfQsLmU6czp50sJwTnsbXuXNF1/view?usp=drive_link

---

**OUTLINE OF COMPLAINT**

---

Background of Compalint surrounds an approximately $6500 USD transfer of Crypto Currency (at time of this writing 8.9BNB coin at approximately $800 USD a coin) from MEXC to FOREX DAX CAN ULC being knowingly, and intentionally stolen. Both entities working in collusion with one another.

The transfer was initiated from MEXC to CRYPTO.COM

**Proof of Transfer**
BlockChain verification number of this transfer to CRYPTO.COM (FORIS DAX CAN) is

REV 1.1 – During review today noticed I had the incorrect transaction number. Corrected with proper transaction number for the BNB chain.

0xa5fece5f0b357621a8351b5d0ab60dfc19cade2edbdab1e859a66286a9d8aa50

/END SECTION REV 1.1

BNB Blockchain Explorer for verification of transfer – BSCSCAN.COM – Link - BNB Smart Chain (BNB) Blockchain Explorer

Image of BlockChain crypto transfer of BNB coin
LINK to external drive for image
→ https://drive.google.com/file/d/1DJkVS3T_-VTpAmHRzM7qIQsth0xa5fece5f0b357621a8351b5d0ab60dfc19cade2edbdab1e859a66286a9d8aa50M81kbuA/view?usp=drive_link

Arrival of BNB coin showing as "pending" at Crypto.com. (This image also shows when I purchased BNB coin at Crypto.com to outline they are now intentionally forcing people to transfer BNB coin to selected exchanges to potentially further this goal. Initial purchase of BNB coin at Crypto.com is at the bottom of the image)
IMAGE 1
→ https://drive.google.com/file/d/1re0tMOfXv4uXrP5JI515W6V5KSIM2Z7q/view?usp=drive_link
IMAGE 2
→ https://drive.google.com/file/d/15dvs0OPK15pvhHrTTlYAt607CidBfyMO/view?usp=drive_link
IMAGE 3
→ https://drive.google.com/file/d/1-CSZ06zbT_0JjpfR6WDTensAdyvpIKzl/view?usp=drive_link

Crypto.com claiming the transfer of 8.9BNB "failed" but I have proof the transaction was accepted and moved out of Crypto.com to a different wallet not tied to me, where billions have moved through.
IMAGE 1
https://drive.google.com/file/d/1LPjt-R1vz4CEQNzyPUpr8xfYTJLM4DAB/view?usp=drive_link

---

**ILLEGAL MOVEMENT OF MY FUNDS, MOST LIKELY OTHERS AFFECTED**

---

Discussion between Crypto.com support claiming the 8.9 BNB coin did not make it to Crypto.com
OSC and RCMP can request these logs under my Crypto.com account as two Chat IDs
Crypto.com Full Name – Mark Lepore
Crypto.com Phone Listed as – 519-341-4125
Crypto.com Email Lised as lepore.mark@gmail.com
Chat ID
5d54d409-5e05-49b9-902e-d281c9aba25f

3e6484eb-7f68-4e60-9f1f-65545ba08282

OVERVIEW OF THESE TWO DIFFERENT SUPPORT REQUESTS EVENTUALLY IGNORED
https://drive.google.com/file/d/1KA23_yAtFlDfrEAGlVC270KxgHXqzhZx/view?usp=drive_link

Direct discussion with Crypto.com support agents deceptive and lying about funds being returned. Offered no legitimate explanation. Did not provide a return transaction hash. You cannot “fail” a transaction on the blockchain, so they were lying to me, and I made them expressly admit it. Crypto.com falsifying where the money was sent and falsified the transaction hash.

IMAGE 1
→https://drive.google.com/file/d/17D_Fe9BrXlsLCVuGj08Atpa1TuH4v4wq/view?usp=drive_link
IMAGE 2
→https://drive.google.com/file/d/1HfvsyWihjyqWU6vWgTFwTVXoNNOB4Rzf/view?usp=drive_link
IMAGE 3
→ https://drive.google.com/file/d/1PMBh5vMt5aTk8NQyXDiDEZ6d728mWjMF/view?usp=drive_link
IMAGE 4
→ https://drive.google.com/file/d/1QBG7YaLgszZh2lkpIZs9Fr4zSuF-GtAK/view?usp=drive_link
IMAGE 5
→ https://drive.google.com/file/d/1RjvV2dM5lsv2wuKjGKMCVEirfFR8EElz/view?usp=drive_link

Discussin number 2
IMAGE 1
→ https://drive.google.com/file/d/1c7SluJSOj2ev69zRILOPu3SF5BSfuCsu/view?usp=drive_link
IMAGE 2
→ https://drive.google.com/file/d/1mrhIKF9sutSEh24w7HlcuEe2bJGchcxF/view?usp=drive_link
IMAGE 3
→ https://drive.google.com/file/d/1kjbrhU2JANKtT1ILQu3s43jdR2ALuFMs/view?usp=drive_link
IMAGE 4
→ https://drive.google.com/file/d/1F9TDqK7MCaEwMptXOIfE0BMv0hmlbL2n/view?usp=drive_link

Reddit Crypto.com support ignored request for explanation →
https://drive.google.com/file/d/1cMHY1l73VghwUPfA_hQD28kpCI17gElA/view?usp=drive_link

REVISON

---

**SPECULATION OF PLANNED AND POTENTIALLY INTENTIONAL FRAUDULENT ACTIVITY.**

---

The reason for the purchase of BNB coin at MEXC is as follows.

I trade on the market, and am aware when a currency “breaks out” it will make rather large moves in the upward direction. The reason for the purchase is because I have full anticipation of BNB coin making a rather large upward movement.

Link for my speculation here as to what will happen. →
https://drive.google.com/file/d/1ZHUxtErV4eiz9WlvOL1s_w_XF5RMrrw_/view?usp=drive_link

Crypto.com seemingly has intentionally blocked purchase of BNB coin, however, I have purchased a small amount of BNB coin in the past from Crypto.com because I anticipated a potential upward spike as mentioned.

Crypto.com has BLOCKED the purchase of BNB coin in the Crypto.com app.

(*NOTE - This is because I believe they are planning on forcing people to move BNB coin out of their exchange to potentially steal their currency, with a potential "pump" of the coin)*.

Planning on this pump up, I moved some ETH to MEXC to swap it to BNB coin and move it back to Crypto.com

Image proving you can **only transfer** BNB coin to an external address (possible planned colusion with other exchanges like Binance to steal more BNB coin? ).

→ https://drive.google.com/file/d/14kGVD0YM-bP_i8ndOo988u9zWbWqwjVG/view?usp=drive_link

Image showing what all other coins have available to them at Crypto.com. You are able to BUY, SELL, and TRANSFER all other listed coins EXCEPT BNB coin. Here is my SOL coin holding with Crypto.com showing how all other coins are able to buy, sell and transfer.

→ https://drive.google.com/file/d/1n-5uP_kc_pyBbWtZNWzNczjwXm5Lc8kd/view?usp=drive_link

The transaction hash for moving my mined Ethereum from Crypto.com to MEXC is here

0x5e9dd086fc59799795b5b642a1694d7b6a4fc8cfabdabe3cbeedacb636afa857

Ethereum blockchain explorer link → Ethereum Transaction Hash: 0x5e9dd086fc... | Etherscan

Link to image of Ethereum transfer of funds from Crypto.com to MEXC

IMAGE 1

→ https://drive.google.com/file/d/1SDN0Wt6ueelnEFdrf9vjCkRIlMszorD4/view?usp=drive_link

IMAGE 2

→ https://drive.google.com/file/d/1PX6srPdwnT0-Tduplxlu7LOJpKEjjBTH/view?usp=drive_link

1.88 ETH DEPOSITED TO MEXC

Ethereum was swapped to BNB coin immediately and transferred back to Crypto.com with the address given above in this document minutes after the funds registered in the MEXC.

IMAGE of MEXC account recent transactions which outline the movement of ETH, purchase of BNB, and transfers. → https://drive.google.com/file/d/1of4lIaaod-FeI6H3AFP2zG4BMhf40RPS/view?usp=drive_link

---

**INTENTIONAL DECEPTION OF CRYPTO.COM**

---

MEXC intentionally removed the transactions after some discussion with Crypto.com about the funds being lost.

→ https://drive.google.com/file/d/1ACSjU0gLpNHsvZlSILQI3sELrJX1jUEr/view?usp=drive_link

MEXC intentionally posting a FALSE transaction hash in their platform with the transfer to Crypto.com after complaints to Crypto.com about the loss of money.

→ https://drive.google.com/file/d/120v69RDFbMDWY0U4-IB8df-lrW10QAz6/view?usp=drive_link

→ https://drive.google.com/file/d/1RAj1trMeIXPmjMwaXk5tRjJdb--6cgLY/view?usp=drive_link

The transaction hash given was as follows which is fraudulent→
0x5e9dd086fc59799795b5b642a1694d7b6a4fc8cfabdabe3cbeedacb636afa857

MEXC removing all traces of the transactions after I copied the false transaction hash.

→ https://drive.google.com/file/d/1OuhQoe2PFcORcJ-JdSF-pIAcnQYVLUAJ/view?usp=drive_link

REV 1.2 - Added now missing withdrawl from MEXC 7-29-25

→ https://drive.google.com/file/d/1SRbSKuwlUMxHwOdGmSwU1v96L2bNnTqc/view?usp=drive_link

/END SECTION REV 1.2

---

**ILLEGAL MOVEMENT OF MY CRYPTO CURRENCY**

---

Here is proof my 8.9 BNB coin made it to Crypto.com and has moved illegally into an external wallet address. This movement must have been made ILLEGALLY by individuals within Crypto.com to an external wallet.

→ https://drive.google.com/file/d/1RY4zzFwks39Y4xy3jPMq_csmVvRpO3Rl/view?usp=drive_link

Illegal transaction address on the BNB blockchain is →
0xc4818ac90feA232Da07c11e972063Bdd7b1e826d

REV 2.1 – ALSO OF NOTE IS A MISSING 0.4663 BNB coin from my account which has been moved somewhere without my knowledge. Also of note, is that it shows the amount which was last in the account, yet I cannot transfer out the coin, as it is not available for transfer. (video and picture evidence provided)

→ https://drive.google.com/file/d/1h5J69gwkLfNgxth5NCHjsjbATRZ7m0JL/view?usp=drive_link

/END SECTION REV 2.1

THE TRANSACTION HASH OF BNB TO MY CRYPTO.COM WALLET CAN BE USED TO BACK TRACK THE TRANSACTIONS TO THESE ENTITIES.

Illegal Wallet with my funds shows several incomming deposits including my 8.9 BNB coin, and movement to external exchanges which are used for loans and money distribution back to unknown entities including MEXC (possible payoffs)

→ https://drive.google.com/file/d/1LKjEzLJ6dAyLe8hgGclkKMNacnLy8u6x/view?usp=drive_link

REV 1.3 – ADDED SCREENSHOT TO SHOW 8.9 BNB COIN IN WALLET ID - 0xc4818ac90fea232da07c11e972063bdd7b1e826d (NOT MY WALLET, SLUSH FUND?)

→ https://drive.google.com/file/d/1eha2vxVMH1fcQW3BFDKvBBzKuunpHvv7/view?usp=drive_link

/END SECTION REV 1.3

MOVEMENT OUT TO TWO ADDRESSES LINKED -

1

LOAN WALLET (VENUS VXS TOKEN) sent to BINANCE, MERCADO BITCOIN, MEXC and other addresses.

It looks like the funds are being moved into VENUS VXS TOKEN to move the currency in the crypto market? MANY exchanges are working together in this. Current wallet amount sits at approximatly $5 million

→https://drive.google.com/file/d/1NanwwrmvfExQeEWOVd-y56qkTcmZeuVW/view?usp=drive_link

→https://drive.google.com/file/d/1MAK3LA69ezVD_c6dUuwWOxa_3OGklFL9/view?usp=drive_link

2

Other external wallet where funds were moved out to showing payments which Binance and other exchanges are contributing to as well. 13 BILLION dollars has moved through this wallet!

→ https://drive.google.com/file/d/1nfhAdqVKkZ9IHAmjgby6gqyagx52QX_q/view?usp=drive_link

REV 1.4 – MULTICHAIN BNB Account. This seems to be a fund where crypto is exchanged to pump markets / make money on known market moves? As a side note… I could have easily exploited this information if my intentions were of malice. I will be making some trades on these currencies at MEXC or Crypto.com… to see what they do… even though my personal money is at risk. I have a feeling I can catch them in more theft. I will report with any additional findings. Feel free to track any movements. I will not be moving "illegally" aquired funds to my personal bank, but will be using about $1000 of my personal money to try and expose additional information. Based on current market moves, I am anticipating these entities to be fraudulently collapsing the system to leave everyone broke, while they launder the money for themselves.

3

MULTICHAIN portfolio with several attached crypto currencies. It seems like they are moving money where profit can be made? Notice CRO Cronos crypto currency is on the list… which is Crypto.com's currency.

→ https://drive.google.com/file/d/1AAUhyknYqbala_DqXz8VKx5WtitbVxTL/view?usp=drive_link

→ https://drive.google.com/file/d/11RTMgVJgqSWygr-_G6JJIIbRqs9e6QBk/view?usp=drive_link

SHIRO COIN is using Almira Wallet deployer, which are clearly all fake accounts meant to hold smaller sums of SHIRO.

→ https://drive.google.com/file/d/1cZbhiomUOuBs3-W_9iNkRwhZmdqUMTQH/view?usp=drive_link

ALMERA Wallet is tied to  KUCOIN and KRAKEN

→ https://www.kucoin.com/ucenter/signup?rcode=QBSSSP3P

→ https://www.kraken.com/sign-up?clickid=2XuRDQ3eWxycRAg2CqxSaQ1mUkp07OWj3ToFwE0&utm_source=Impact&utm_medium=Affiliate&utm_campaign=1981006&utm_content=Online Tracking Link&irclickid=2XuRDQ3eWxycRAg2CqxSaQ1mUkp07OWj3ToFwE0&ref_url_custom=&irgwc=1&mpid=1981006

COIN CODEX seems to be deploying the wallet from here

→ https://coincodex.com/crypto/almira-wallet/guides/

IMAGE OF DEPLOYMENT LOCATION

→ https://drive.google.com/file/d/1S8TtfkVNZOWxr7k9hasxnaYfDB1kuqOT/view?usp=drive_link

/ END SECTION REV 1.4

---

**POTENTIAL LAWS EVADED AND BROKEN**

---

**OSC SECURITIES LAWS**

National Instrument 31-103:

Requires registrants to deal fairly, honestly, and in good faith with clients.

- - National Instrument 31-103, requires fair dealing and transparency.
- - CSA Staff Notices 21-327 & 21-329, which demand proper custody and delivery of crypto assets
- Failure to provide a valid transaction hash, resulting in

  1. - breach of contract

  2 - misrepresentation or fraud

  3 - violation of securities law and AML regulations

**CRIMINAL LAWS**

Section 322 – Theft

Taking property fraudulently and without the owner's consent is a criminal offence. Even temporary deprivation.

- Section 380 – Fraud

Deception used to cause loss or gain, is considered fraud. This includes misleading users about transactions, fees, or account access.

- Section 361 – False Pretences

Making false representations to obtain property or money is illegal—even if I had voluntarily handed it over.

- Section 402.1 – Identity Theft and Identity Fraud

If personal information is misused to access accounts or impersonate users, this section applies.

- Section 347 – Criminal Interest Rate

Charging interest above 60% annually is illegal. If fees or penalties are disguised as interest, this could be relevant.

- Section 462.31 – Proceeds of Crime

Money obtained through theft or fraud is laundered or reinvested, this law targets the handling of those funds.

- Section 21 – Parties to Offences

If two entities are working together, they may be considered co-conspirators or facilitators of the offence—even if only one directly commits the act.

Conspiracy Charges

Under Part XIII, conspiring to commit a crime is a criminal offence—even if the theft or fraud hasn’t yet occurred.