OECD International Academy for Tax Crime Investigation

Investigative Techniques for the Effective Use of Banking Information

OECD

OECD Anti-Money Laundering / Crypto Presentation

Mark Waldon – Senior Investigation Officer HMRC

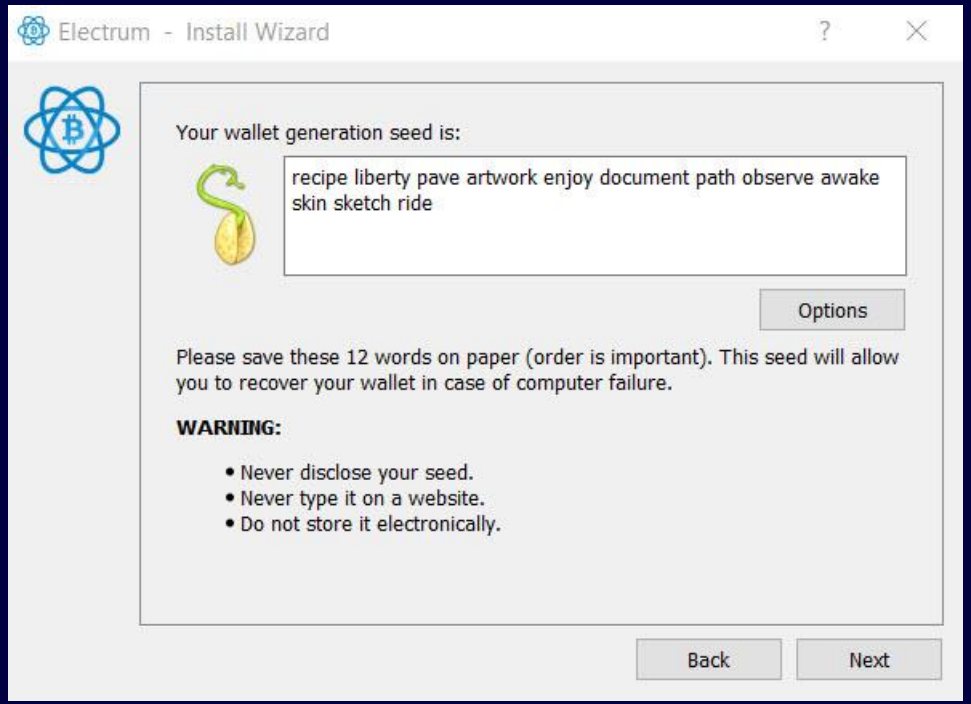
Definitions: Cryptocurrency

- Any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions.

'*Sapiens*' – Yuval Noah Harari

- "The sum total of money in the world is about $60 trillion. More than 90% of all money – more than $50 trillion appearing in our accounts – exists only on computer servers. Accordingly, most business transactions are executed by moving electronic data from one computer file to another"

Cryptography – from the Greek ‘Cryptos’ (to conceal)



Defintions:

Money laundering is the illegal process of making ‘dirty’ money appear legitimate

Criminals have historically used a variety of money-laundering techniques – cash business; cash purchases; small bank deposits; Money Service Bureau’s (MSB)

Online banking and cryptocurrencies have made it even easier for criminals to access their ill-gotten gains without detection

Other definitions….

Proceeds of Crime Act 2002

- Section 327 – concealing/disguising (inc Transferring)
- Section 328 - arrangement
- Section 329 – acquisition, use and possession

- Plus other offences in the UK such as ‘Cheating the Revenue contrary to Common Law’

How is HMRC set up to tackle ML involving Crypto?

- Fraud Investigation Service (FIS)
- Risk and Intelligence Service (RIS)
- Digital Support and Innovation (DS&I)

Surveillance Presentation

To follow

Considerations:

- Can I obtain the information / evidence by another less intrusive and resource intensive method?
- Do I have adequate resources and assets at my disposal in order to conduct surveillance without compromising the operation and/or individuals?
- Has my team been properly trained and briefed?
- Area/s of operations – sensitivities, exposure to LEA methodology
- Use of technical solutions by LEA – camera cars, local CCTV, bank CCTV etc

Techniques

Profile

- Where are you conducting your surveillance?
- Where is the subject likely to go/visit?
- Build into your planning the ability to improvise

Use of vehicles

The Goal….

The ultimate aim of surveillance is to follow your subject to a place where he/she will interact with others and/or carry out tasks related to your investigation

Preparation for surveillance

- Am I authorised to conduct this activity?
- Area of operations
- What is already known?
- Can you ‘plot’ ahead? – have someone inside the venue?
- Actions on? Are we taking the known subject away or the new subject?
- Resources? People, vehicles, equipment….
- Briefing, RV, ERV, debrief

Post-Surveillance

- Operational security – any compromises?
- Intelligence / evidence gained
- Overheards, recordings, photographs
- Actions on new information – bank employee
- Name; address; DOB; information held by other government departments / bank; Criminal record; vehicles owned; relationships
- Decide whether she/he is an active subject of the investigation OR can she be ‘flipped’ as an informant/participating informant. If the latter can she introduce an undercover operative? If she is to become an informant, is she robust enough to handle it? Could she undergo witness protection measures? Etc etc….
- Plenty to consider…….

Technical & other solutions…

- Use of an OP (Observation Point) – apartment, business, farm etc
- Use of technical – covert cameras, audio recording devices, body worn devices
- Application to local authorities for CCTV footage
- Drones

In the UK we would be entering into a world of new and higher levels of authority for use of the above than we would when conducting conventional physical surveillance.

Covert methods of surveillance

AS/CS

- Anti-Surveillance is conducted in order to ascertain whether you and/or your team are being watched

- Counter Surveillance is the art of ‘watching those who are watching you’

DS&I

- Covert Operations inc:
- Central Authorities Bureau (CAB)
- Covert Operations Management Unit (covert planners)
- Command & Control
- Tactical Surveillance Group
- Protected Persons Unit (PPU)
- National Digital Investigation Unit
- Undercover Unit
- Close & Near Exploitation Team (CNET)
- Comms data





DSI : UNDERCOVER UNIT

Open Source tiered operating model

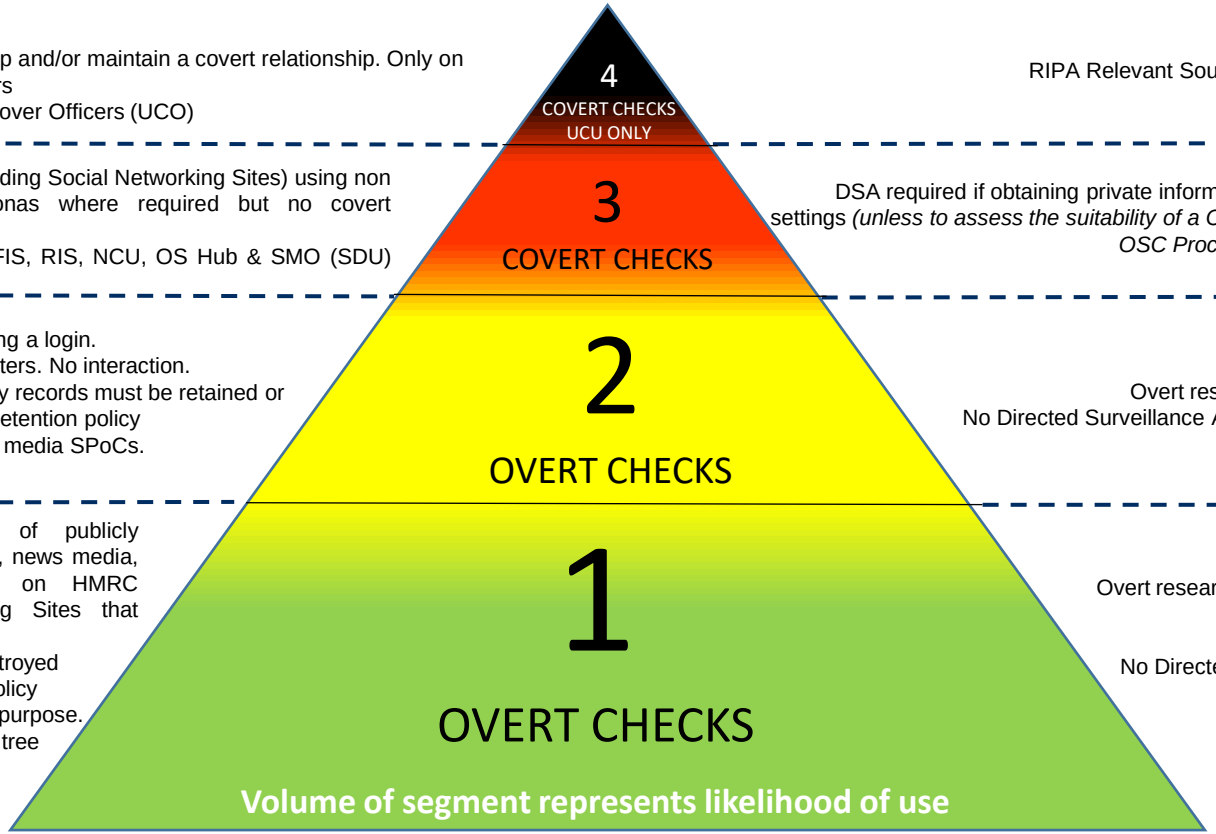
How? Who?

How: Use of false persona to develop and/or maintain a covert relationship. Only on authorised non attributable computers
Who: only authorised Online Undercover Officers (UCO)

How: Covert Internet research (including Social Networking Sites) using non attributable computers and personas where required but no covert relationship. No two way interaction.
Who: Only Digital Investigators in FIS, RIS, NCU, OS Hub & SMO (SDU) trained staff.

How: Overt internet research requiring a login.
Using HMRC credentials and computers. No interaction.
Must not breach privacy settings. Any records must be retained or destroyed in accordance with local retention policy
Who: A network of authorised social media SPoCs.
Mandatory training required

How: Overt Internet research of publicly accessible information, street views, news media, business sites, GOV.UK sites, on HMRC computers. No Social Networking Sites that require a login.
Any records must be retained or destroyed in accordance with local retention policy
Who: All HMRC staff for any HMRC purpose.
Follow Tier 1 guidance and decision tree



Authority

RIPA Relevant Source authority mandatory.

DSA required if obtaining private information or breaching privacy settings *(unless to assess the suitability of a CHIS where RIPA CoP and OSC Procedures & Guidance apply)*

Overt research requiring a log in.
No Directed Surveillance Authority (DSA) required

Overt research of publicly accessible areas of the Internet

No Directed Surveillance Authority (DSA) required

Deploying an Undercover Officer online

- What might that officer need?

- Please break into groups to discuss what you would have in place for a safe, legal and successful deployment

Undercover Presentation

To follow

UNDERCOVER

The Undercover Unit is responsible for, and manages all, departmental undercover operations, providing advice to all areas of HMRC in relation to the potential opportunities for undercover deployments. It acts as a single point of contact with other agencies who support HMRC in such activity and can reciprocate support to those agencies in respect of their own undercover activities.

Undercover Operatives

UCOs are members of a law enforcement agency who are selected, vetted, trained and accredited to gather intelligence and evidence.

There are three categories of UCO:

1. Undercover **foundation** operatives (UCFs)

2. Undercover **advanced** operatives (UCAs)

3. Undercover On- line only (UCOLOs)

Regulation of Investigatory Powers Act (RIPA) 2000

- A person who establishes or maintains a personal or other **relationship with another** person for the **covert purpose** of facilitating anything that:

- **covertly uses** such a **relationship to obtain information** or to provide access to any information to another person; or

- **covertly discloses information** obtained by the use of such a relationship or as a consequence of the existence of such a relationship

PHYSICAL DEPLOYMENTS

- Opportunity infiltrations - usually used where the targets are actively seeking certain services we can provide.
- Proactively targeted infiltrations - in the main focussed on the infiltration of certain groups/individuals.
- HUMINT/CHIS infiltrations - normally these are deployments from initial introductions by CHIS sources into criminal groups.
- Covert acquisition of premises/vehicles to use as a platform for further DS&I technical opportunities.

Legend Businesses

- Fruit and veg importer and distributor
- Accountancy and Taxation services
- Property Management
- Freight and Customs clearance agent
- Clothing Importer and distributor
- Vehicle trader
- Various trading platforms

COUNTER AVOIDANCE

Support to Counter Avoidance Directorate in attempting to establish if webinar and/or seminar events hosted by various organisations were promoting tax avoidance schemes which should be disclosed under Disclosure of Tax Avoidance Schemes (DOTAS) legislation.

Tax under consideration due to UC activity in excess of £300 Million.

Warehouse theatre

Warehouse theatre

Operation I ********** – Close Access

- To obtain an office adjacent to the subjects.
- To carry out a pattern of life to facilitate covert entry.
- To undertake a security survey.
- To obtain subjects alarm code.
- To provide secure front end recording.
- To provide a cover story for NCA MoE team and NCA/HMRC techies.
- Premises rental required relevant backstopping and theatre .
- Utilised a fruit and veg import company.
- Rental required bank references and public liability insurance.
- Needed to import from China to maintain integrity.
- 8 covert entries made’
- Exit strategy.

HM Revenue & Customs

Operation I ********** – Close Access

Apple Desktop

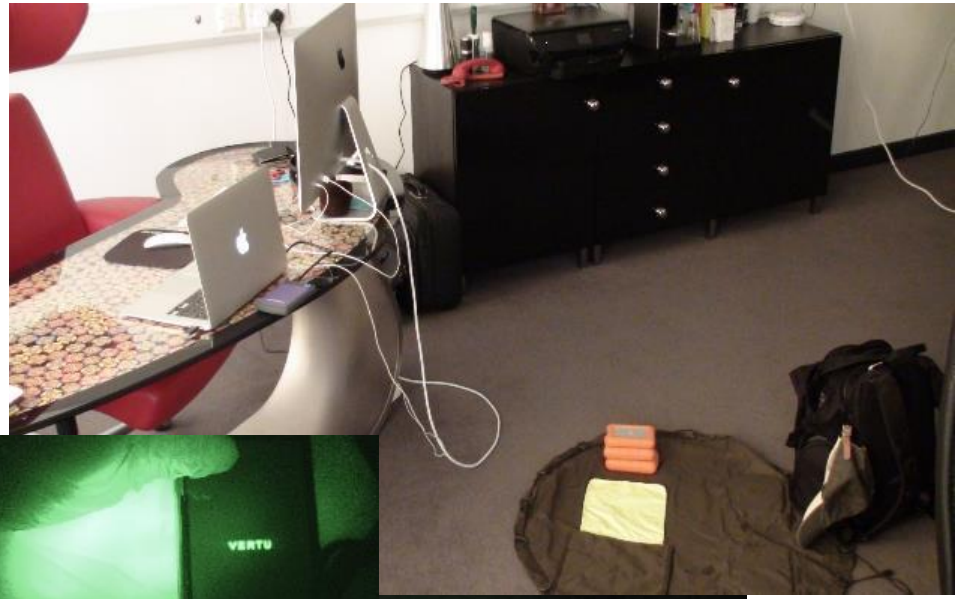
Apple Laptop

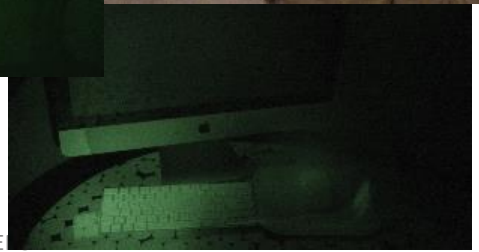
Printer

Router

USB Hard Disk

Vertu Mobile Phone





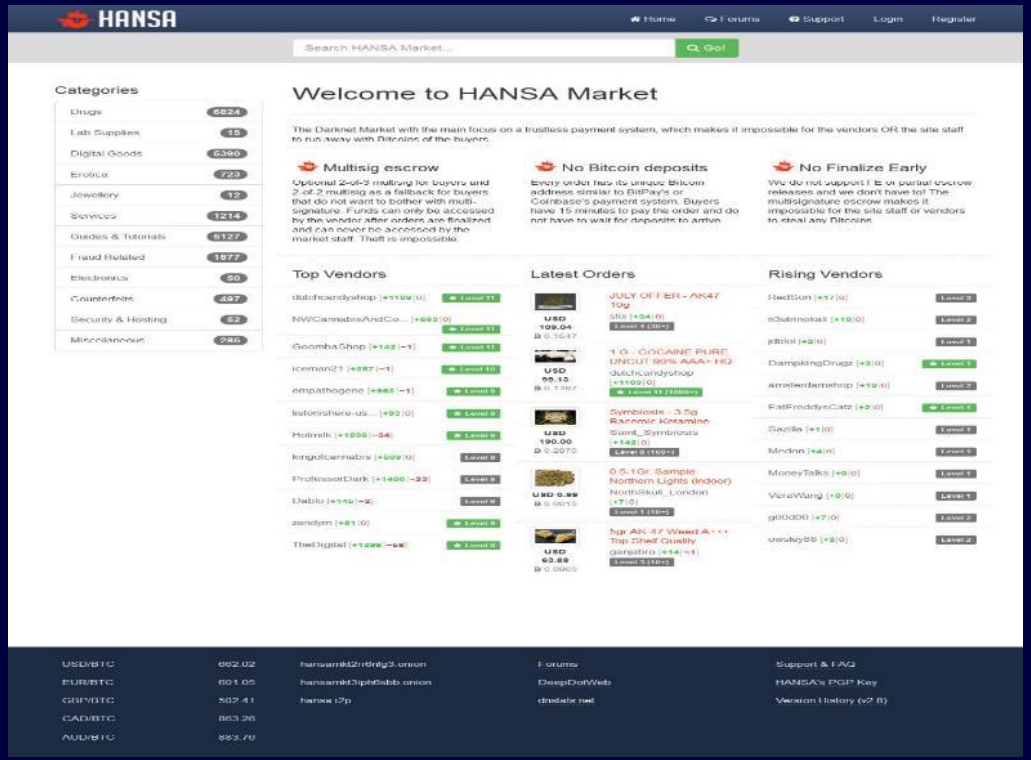
- 1,390,737 Emails (5468 unique addresses)
- 70 Backups of smart devices (phones & tablets)
- 1,500 Calendar Appointments
- 33,000 SMS
- 142,000 Documents
- 25,859 Spreadsheets
- 415,000 Images

Legend Building

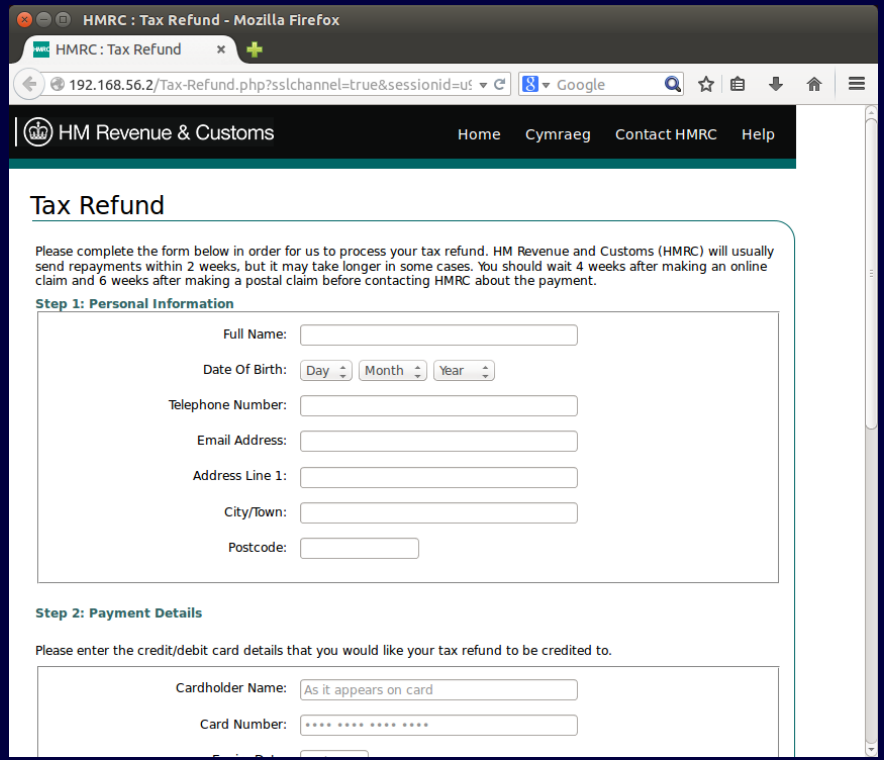
- Authority
- Proof of address, DOB, passport/driving licence, bank account
- Phone / laptop
- Crypto wallet
- Cold wallet?
- Online presence – surface web
- Darknet presence
- Social media footprint
- A company?

Undercover activity was undertaken in the ‘Dark web’ by trained UCOL’s

Early deployments onto the Darknet

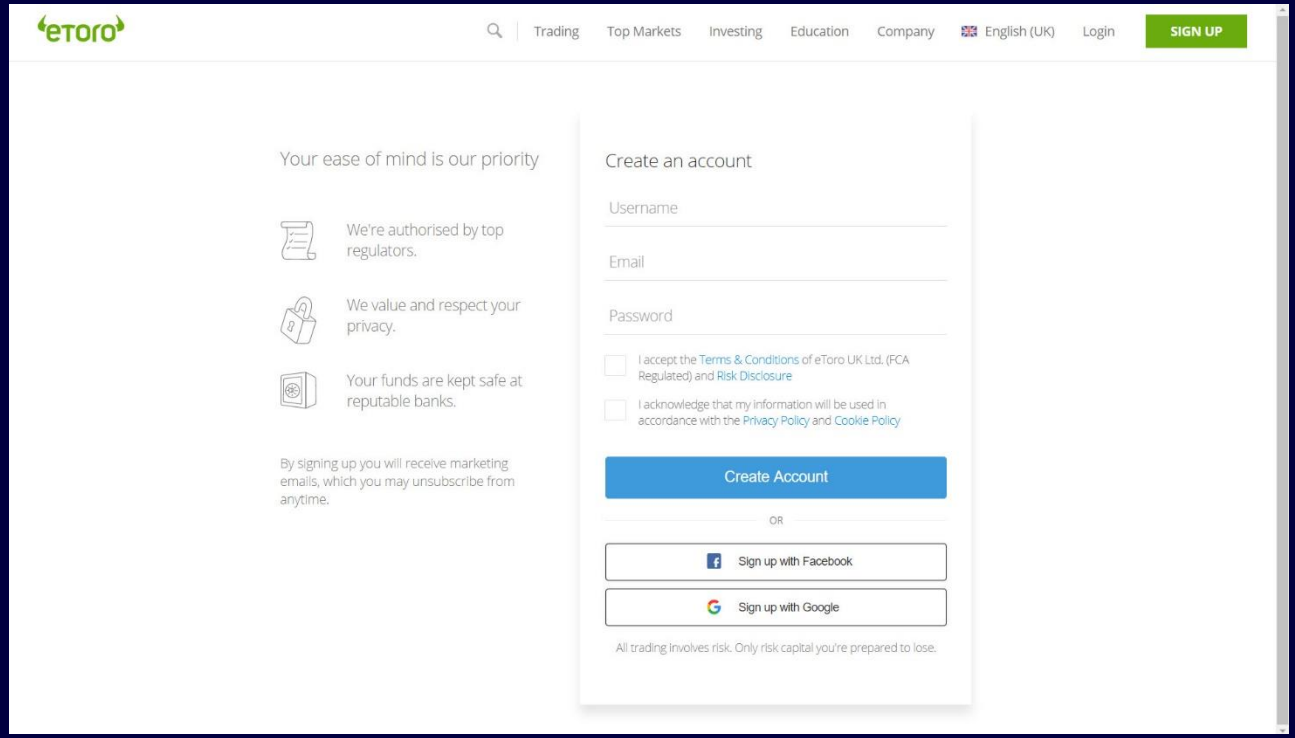


Finding Fraud scams



UCOs operate numerous cryptocurrency accounts

The ‘Ramp on’ to holding and exchanging cryptocurrency



Changing / emerging patterns

- Compliance around Crypto ATM's increased and tightened
- The Financial Conduct Authority (FCA) began a registration scheme for ATM's requiring KYC
- Sites such as Coinradar were used to find ATM's began to see usage fall
- 2 risk areas came to the fore as a result – Face2Face (or P2P) and smurfing

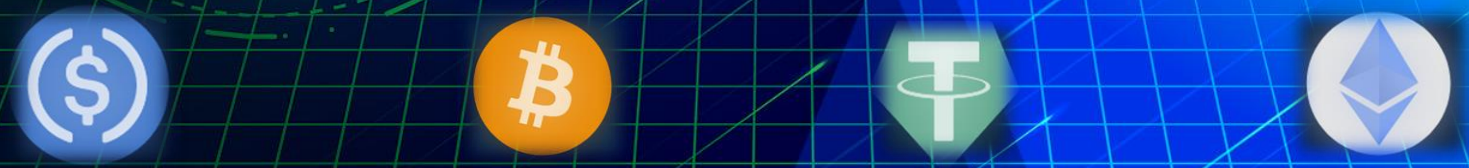
Smurfing

- A type of money laundering conducted by money mules known as ‘smurfs’ who structure large amounts of cash into multiple small transactions
- All calculated to avoid triggering financial AML protocols
- Labour intensive with associated risks and overheads

Smurfing 101

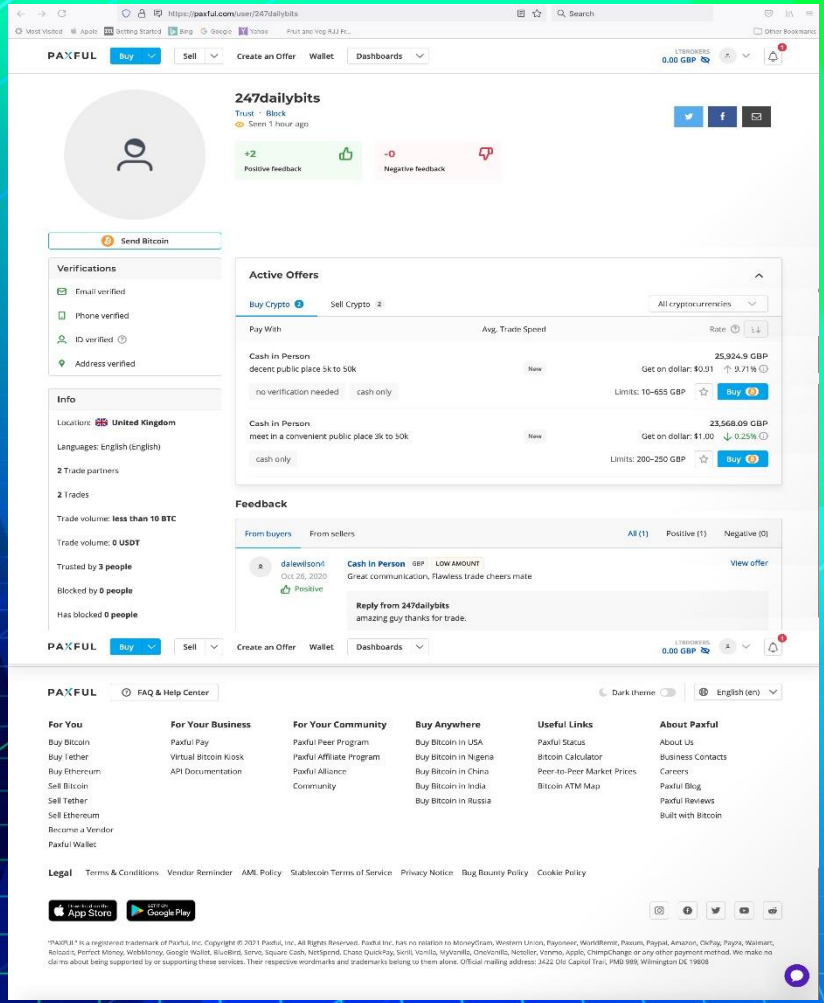
Background to F2F

- Face to Face and/or Peer to Peer (P2P) Crypto trading identified as high risk area for facilitation of ML using Crypto Assets.
- Surface web P2P trading platforms facilitate buying and selling of Crypto via Escrow or face to face cash transactions – little or no KYC required.
- P2P trading preferred method for OCG's over Crypto ATM's – larger amounts possible and borderless, less KYC.



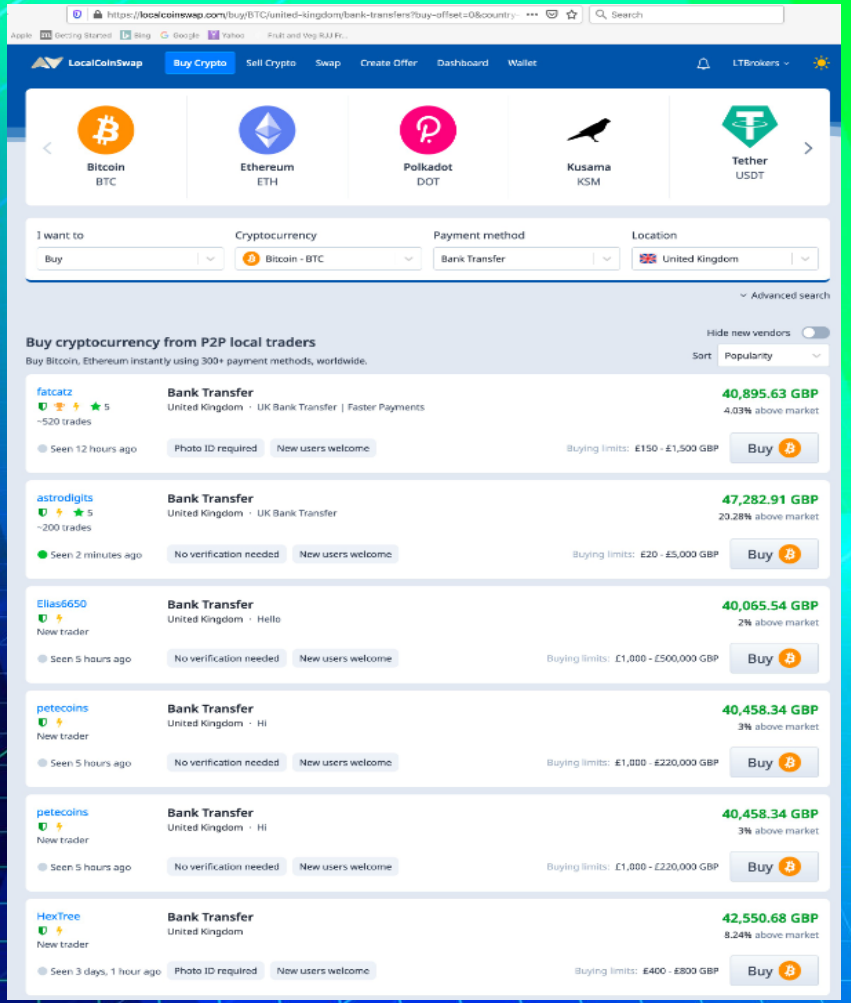
P2P Trading Platforms

Paxful.com (example trade posting from user 247dailybits)



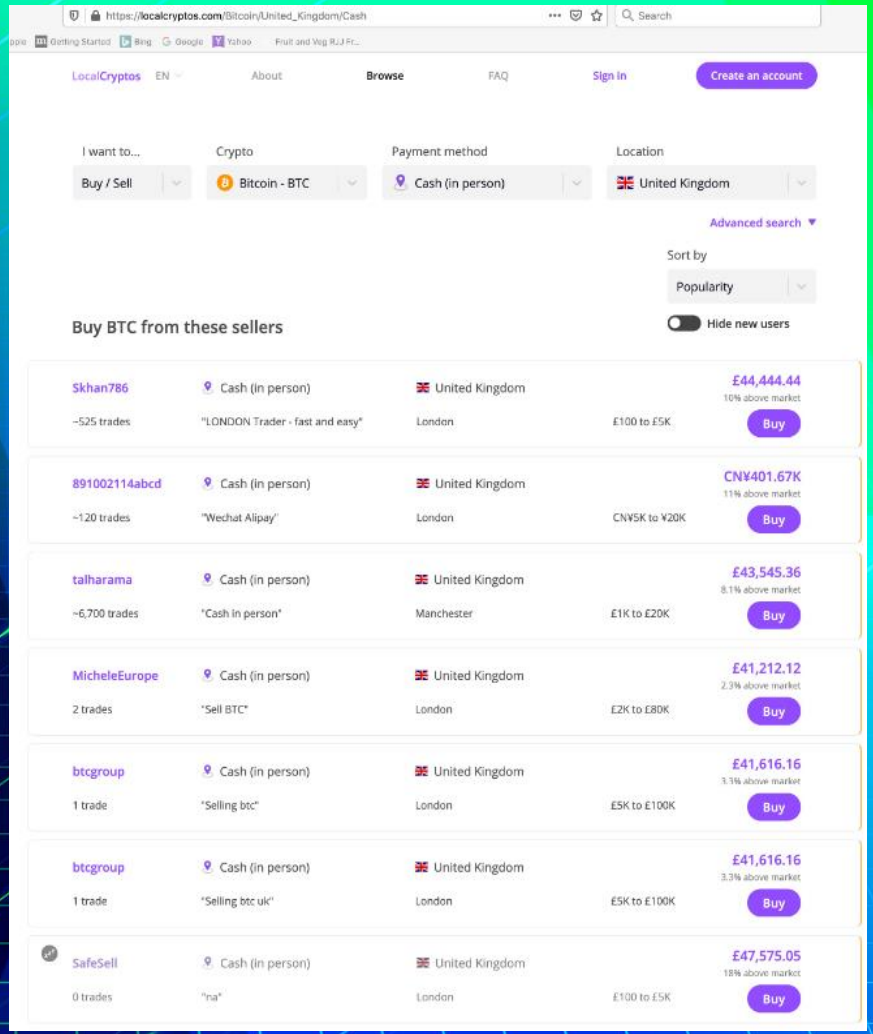
P2P Trading Platforms

localcoinswap.com (example of vendor listings to sell BTC via bank transfer)



P2P Trading Platforms

localcryptos.com (example of vendor listings to sell BTC cash in person)



Operation Chimera

Peer to Peer (P2P) Cryptocurrency Trading

Background

- Face to Face and/or Peer to Peer (P2P) Crypto trading identified as high risk area for facilitation of ML using Crypto Assets.
- Surface web P2P trading platforms facilitate buying and selling of Crypto via Escrow or face to face cash transactions – little or no KYC required.
- P2P trading preferred method for OCG's over Crypto ATM's – larger amounts possible and borderless, less KYC.
- One individual in particular, Sammy Burnett, believed to use P2P trading to facilitate large scale ML.

Tasking

- Tasking received from RIS IDT to research via open source P2P Crypto trading platforms where Burnett believed to operate.
- Register accounts online with main P2P platforms.
- Carry out number of legend building trades to build credibility/knowledge.
- Engage and trade/exchange crypto with principal suspect Burnett aka @mrsammyonline & @247dailybits.

Activity

- Established new legend with associated banking, clean mobile phone.
- Registered accounts on principal trading platforms. Set up number of crypto wallets, including cold wallet. Exchange account set up to repatriate crypto back into fiat currency.
- Carried out number of legend building transactions buying BTC from 3rd party vendors via bank transfers utilising platform Escrow services and hot wallet.
- Contact made with Sammy Burnett on associated Telegram handle @BTCAllday to arrange initial face to face ‘off platform’ purchase of £5K worth of BTC for cash.

Activity

- Number of further face to face trades carried out with Burnett to build trust and maintain credibility.
- Built up to monthly trades of £20-£25K per trade, principally buying BTC for cash.
- Carried out reverse trade, selling £25K of BTC to Burnett for cash.

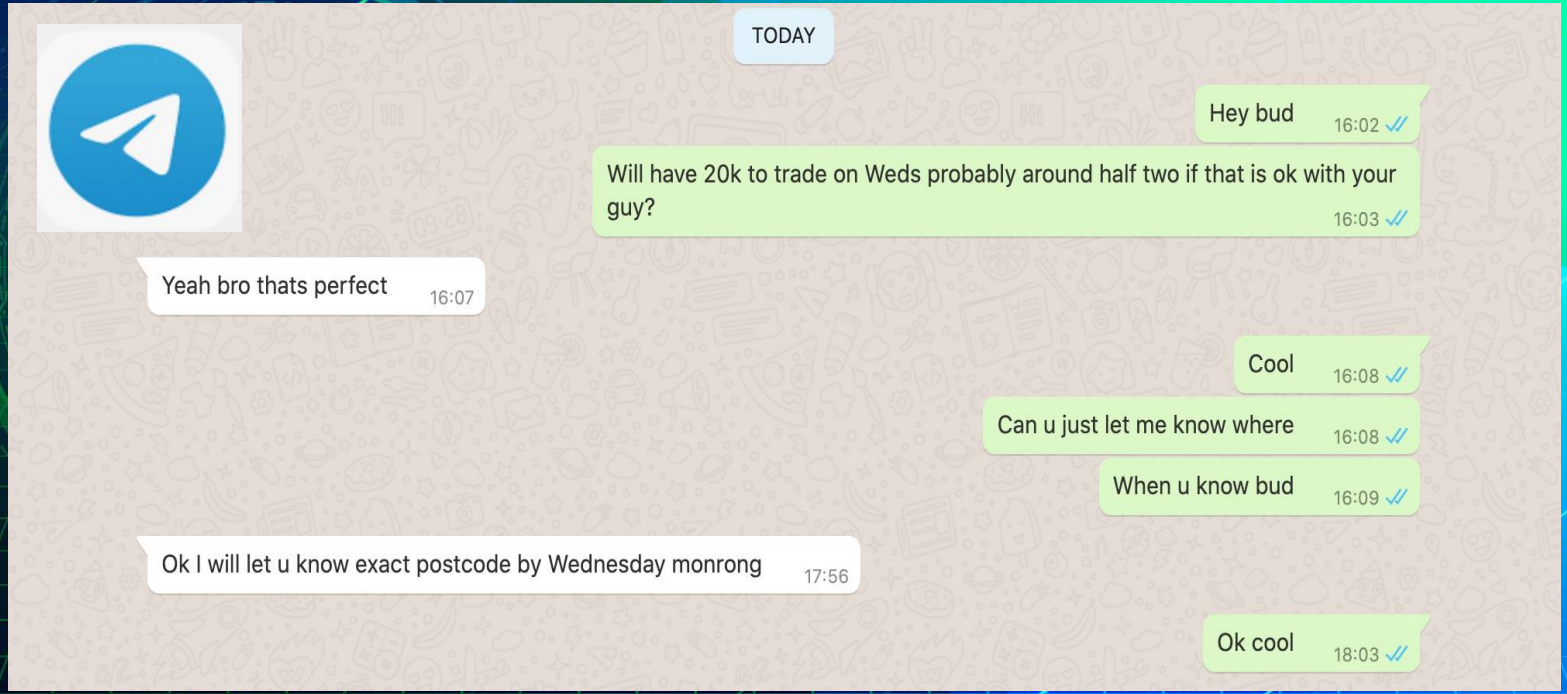
Trade – 5th January 2022

- During a previous trade in December 2021 Burnett offered up a trusted UK associated to collect cash from UC, in the event that he was out of the UK. Burnett would still transfer the BTC to UC but remotely.
- UC tasked with carrying out trade to identify associate.
- UC arranged to trade on 5th January 2022 for purchase of £20,000 cash of BTC whilst Burnett was in Dubai.




31/12/2021 –Initial Contact

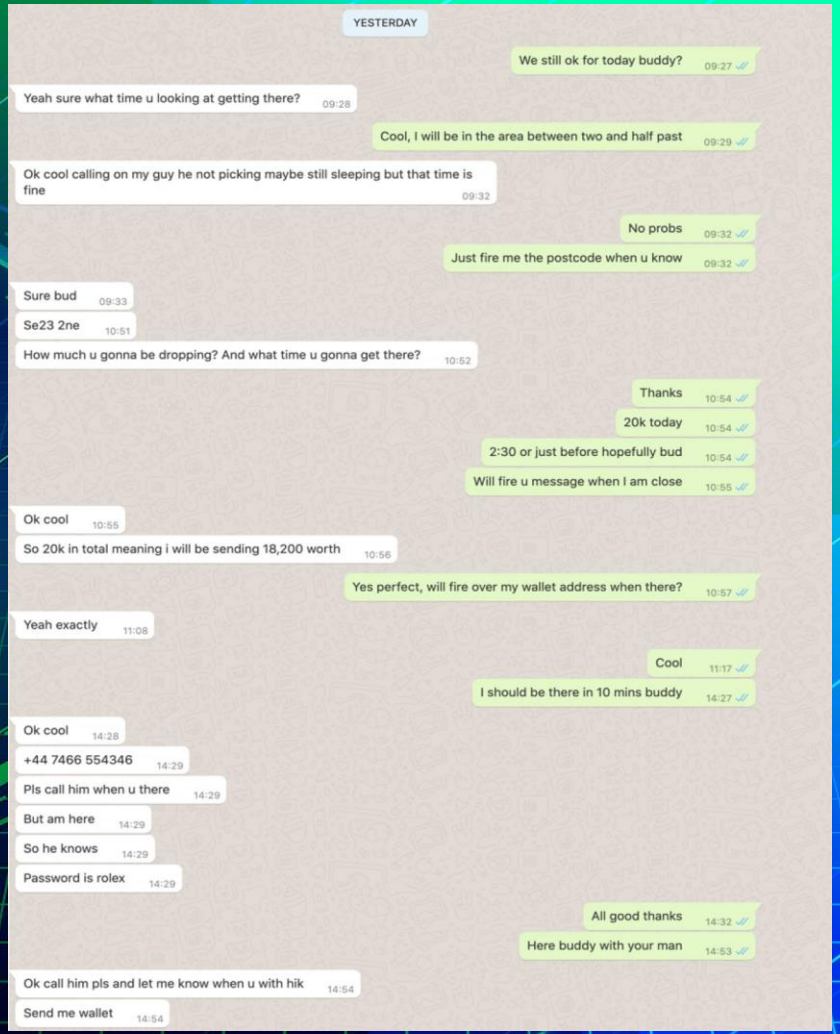
03/01/2022- Confirmation



05/01/2022 –

Leading up to Trade

meet/trade



Intelligence/Evidence Gathered

- Modus Operandi of Burnett ML activities – commission rates for P2P trades and for his ML services to overseas associates. Potential large amounts of cash stored at his home address.
- Identification of crypto wallets and associated devices used by Burnett – Binance, Exodus, Blockchain. Wallet balances in excess of £400k at any one time.
- Identification of Dubai associate for which Burnett receives large amounts of ‘street cash’ and converts to crypto.
- Identification of UK associate along with MSB’s used by Burnett in furtherance of his criminal activities.

Enforcement Action

- What is the predicate offence?
- Are there any other offences to take into consideration?
- Assets and forfeiture. What are your strategies?
- Tactical plan around search and seizure upon arrest?

Arrest and court preparation

- Money laundering contrary to POCA
- Tax offences
- Intelligence linking the subject to cash derived from gun crime and drug/tobacco smuggling
- Cars, watches and significant amounts of cash seized
- Phones and laptops seized for evidential exploitation

Non Fungible Tokens (NFT's)

- Decentralized and relatively unknown space
- Easy to set up non-attributable wallets via web and phone Dapps
- Blockchain analytics not yet compatible with NFT's
- Access via Peer 2 Peer and DEX integration (decentralized exchange)


Be
Brilliant