Forming the suspicion: the DPT typologies

Dr Alexander Ressos, TEP
Attorney-at-Law (Switzerland and Germany),
Solicitor (England & Wales and Hong Kong)
Of Counsel, KGP Legal LLC
alexander.ressos@kgplegal.com.sg
www.ressos.com.sg

What makes a DPT transaction suspicious? The FATF's red-flag indicators of September 2020 and the ACIP typology papers give the taxonomy, and MAS expects a firm's monitoring rules and analyst training to reflect it.[1] The indicators that recur in Singapore practice are the following. Structuring of fiat deposits or DPT purchases just below internal thresholds. Rapid conversion of deposited fiat into DPTs and immediate withdrawal to an external wallet, with no trading in between, which is the classic on-ramp for scam proceeds. Receipt of DPTs from addresses that analytics tools link to mixers, darknet markets, sanctioned entities, ransomware or hacked exchanges. Inbound transfers from many unrelated addresses consolidated and withdrawn to one. Use of privacy coins or chain-hopping across bridges. Customers whose declared occupation and income cannot support the volumes. Customers who are evasive about the source of tokens or whose explanations change. Transactions inconsistent with the stated purpose of the account.

Scam proceeds dominate Singapore's STR picture. The Singapore Police Force reported scam losses of several hundred million Singapore dollars a year from 2021 onwards, with a large share of victims' funds exiting the banking system through DPT exchanges.[2] The typical pattern is that a victim is induced to transfer fiat to a

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

mule account or directly to a DPT exchange account in their own name, to buy stablecoins and to send them to an address controlled by the scammer. From the exchange's side the customer is the victim, the deposit comes from the customer's own bank account and the withdrawal goes to an address the customer declares as their own. The red flags are subtle: a new customer, a first-time buyer, a large purchase relative to declared income, an immediate withdrawal, a destination address that analytics tools associate with known scam clusters. Sometimes the customer is on the telephone during the onboarding video call. MAS has pressed DPT licensees to intervene in exactly these cases, through transaction delays, warning messages and outbound calls, and treats a firm's scam-intervention statistics as part of its AML assessment.

Example

A Singapore DPT exchange onboards a 62-year-old retired teacher who declares annual income of S$ 30,000 and savings of S$ 400,000. Within a day of onboarding she deposits S$ 180,000 from her own bank account, buys USDT and instructs withdrawal to an address she has declared as hers, proving control by signed message. The analytics tool shows the address is fresh. Nothing in the transaction is unlawful on its face. The combination of age, first transaction, size relative to income, immediate withdrawal and a fresh address matches the scam typology in the firm's risk assessment. The firm's policy requires a hold and an outbound call. The call reveals that she is "investing with an adviser she met online" who told her to open the account. The firm declines the withdrawal, explains why, and files an STR identifying the destination address. The customer is angry. Three weeks later she thanks the firm. The STR, the call note and the hold are the file that shows MAS the monitoring works.

Notes

1. FATF, Virtual Assets: Red Flag Indicators of Money Laundering and Terrorist Financing, September 2020, grouped into indicators related to transactions,

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

transaction patterns, anonymity, senders and recipients, source of funds and geographical risks. ↩

2. Singapore Police Force, Annual Scams and Cybercrime Brief 2023 and 2024, reporting total scam losses and the proportion of cases involving conversion to cryptocurrency. ↩

Disclaimer

This article is provided for general information only. It is based on publicly available sources as at its date of publication. These sources have not been independently verified against licences, regulatory registers or the records of the entities concerned. It is not legal, tax, financial or investment advice. Nor is it a recommendation to invest in, transact with or use the services of any entity mentioned. Law and regulation change frequently, so the content may be incomplete or outdated. To the fullest extent permitted by law, Dr Alexander Ressos and the publisher of SingaporeIQ exclude all liability for loss or damage arising from the use of or reliance on this article. Readers should obtain advice on their specific circumstances before acting or refraining from action.

Names and trademarks of the entities discussed belong to their owners and are used for identification only. Their mention implies no endorsement, affiliation or allegation of wrongdoing. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. Corrections and updates: contact@ressos.com.

© 2026 Dr Alexander Ressos. This article may be quoted with attribution to SingaporeIQ (SingaporeIQ.com). Reproduction in full and any commercial use require prior written consent. The Legal Terms at https://singaporeiq.com/legal-terms apply.

Author contact: Dr Alexander Ressos, TEP · contact@ressos.com