Research Papers

August 2026

North Korean Crypto-to-Fiat Activity

Allison Owen and Noémi També

RUSI

Disclaimer

The content in this publication is provided for general information only. It is not intended to amount to advice on which you should rely. You must obtain professional or specialist advice before taking, or refraining from, any action based on the content in this publication.

The views expressed in this publication are those of the authors, and do not necessarily reflect the views of RUSI or any other institution.

To the fullest extent permitted by law, RUSI shall not be liable for any loss or damage of any nature whether foreseeable or unforeseeable (including, without limitation, in defamation) arising from or in connection with the reproduction, reliance on or use of the publication or any of the information contained in the publication by you or any third party. References to RUSI include its directors, trustees and employees.

RUSI Research Papers, August 2026

ISSN 2977-960X

Publications Team

Editorial

Director of Publications: Alice Trouncer

Managing Editor: Sarah Hudson

Assistant Editor: Sophie Boulter

Assistant Editor: Liz Ottosson

Design

Graphic Designer: Lisa Westthorp

Research Editorial

Head of Research Governance and Editorial: Elias Forneris

Cover image: Ink Drop / Alamy

Get in touch

www.rusi.org

enquiries@rusi.org

+44 (0)207 747 2600

The Royal United Services Institute for Defence and Security

61 Whitehall, London

SW1A 2ET

United Kingdom

Follow us on

Contents

1 **Data Provider Statement**
1 Disclaimer

3 **Executive Summary**

4 **Introduction**
5 Definitions

6 **VA-to-Fiat Conversion in North Korean Money Laundering Schemes**
9 Communication Patterns Relevant to North Korean Activity
11 Small Transaction Amounts
12 Money Mules
13 Other Proliferation Finance Identifiers
15 Analysis of PF Indicators in Table 3
17 The Fiat Currency Side

21 **Private Sector Practices and Compliance Measures for VA-to-Fiat Conversion Services that Can Strengthen CPF**
21 Observed Private Sector Practices for Financial Institutions
27 Observed Private Sector Practices for VASPs

32 **Conclusion and Key Recommendations**

34 **About the Authors**

Methodology

Research for this paper was conducted between September and December 2025. This research combines three sources of data. Primary data is derived from a literature review, including Financial Action Task Force (FATF) documents, guidance from Virtual Asset Service Provider (VASP) regulators and supervisors, reports from international bodies and the private sector.

Secondary data on North Korea-linked indicators is taken from 25 semi-structured interviews – conducted between September and November 2025 – with representatives of the following companies and agencies based in the US, Europe and Asia:

- VASPs (4 interviews)
- virtual asset (VA) investigation company (4)
- anti-money laundering (AML) compliance specialist (3)
- financial institution (3)
- cybersecurity specialist (2)
- VASP supervisory authority (2)
- financial intelligence unit (FIU) (1)
- AML investigations company (1)
- law enforcement (1)
- prosecutor (1)
- VA-related company (3).

Each interview incorporated one of four questionnaires, depending on whether the representative's experience is in a traditional financial institution, a VASP, North Korea investigations or the public sector. Interview responses are coded for anonymity to enable candid disclosure of information. For two companies, the interviewees requested to be named and verified statements, and therefore, the company names are listed. To verify specific information acquired from interviews, a blockchain analytics provider, Elliptic, acted as a data provider, sharing insight on requested topics relating to North Korea indicators.

The paper was submitted on 15 April 2026 following validation from stakeholders and approved for copy-editing on 7 July 2026. The research faces limitations with respect to differentiating North Korea indicators from those of third-party facilitators. This is due to overlaps in the money laundering networks.

While the authors strive for accuracy and quality, note that the information provided may not be entirely error-free or up to date. RUSI does not assume any responsibility or liability for the use or interpretation of this content.

Data Provider Statement

The authors would like to thank Tom Robinson and the research team at Elliptic for providing data from internal investigations and analysis on requested topics. This analysis supported validation and expansion on interview responses for this research paper.

Disclaimer

The content in this publication is provided for general information only. It is not intended to amount to advice on which you should rely. You must obtain professional or specialist advice before taking, or refraining from, any action based on the content in this publication.

The views expressed in this publication are those of the authors, and do not necessarily reflect the views of RUSI or any other institution.

This document has been prepared by RUSI for informational purposes only (the 'Permitted Purpose'). While all reasonable care has been taken by RUSI to ensure the accuracy of material in this report (the 'Information'), it has been obtained primarily from multilateral and unilateral government reports, private sector reports, or third-party providers and RUSI makes no representations or warranties of any kind with respect to the Information.

You should not use, reproduce or rely on the Information for any purpose other than the Permitted Purpose. Any reliance you place on the Information is strictly at your own risk. If you intend to use the Information for any other purpose (including, without limitation, to commence legal proceedings, take steps or decline to take steps or otherwise deal with any named person or entity), you must first undertake and rely on your own independent research to verify the Information. To the fullest extent permitted by law, RUSI shall not be liable for any loss or damage of any nature whether foreseeable or unforeseeable (including, without limitation, in defamation) arising

from, or in connection with, the reproduction, reliance on or use of any of the Information by you or any third party. References to RUSI include its directors, trustees and employees.

For this report, the names of companies listed represent information from one of three categories: they are listed in in multilateral or unilateral government reports; they have been documented by private sector entities; or the names have been provided by a third-party provider.

Executive Summary

Between January 2024 and September 2025, North Korea is estimated to have stolen at least $2.8 billion in virtual assets (VAs). These funds are assumed to directly support its WMD programme. The methods used to launder these funds through decentralised services are well documented. However, research has only marginally addressed behaviours of North Korea-linked actors at the nexus of blockchain-based and traditional financial systems. Efforts need to consider the larger picture of how stolen virtual assets integrate into broader sanctions evasion activity. Specifically, better visibility of the behaviours that enable the conversion of VAs into fiat currency is one component in a complex network that, when understood, can help to limit the regime's access to the proceeds of cybercrime. This paper focuses on North Korean behaviour at VA exchanges. Building on this insight, the paper outlines key areas that the private sector should consider to address vulnerabilities. These are foundational gaps that, once resolved, help to streamline investigations involving multiple financial crime types, including proliferation finance.

This paper also provides key considerations for policymakers. Implementation of these recommendations can support the industry with closing identified gaps:

- Regulators should consider issuing clear guidance on how correspondent relationships between virtual asset service providers (VASPs) – that is, arrangements where one VASP provides services or access to financial infrastructure on behalf of another – are to be managed, particularly when interacting with unlicensed VASPs.
- An International Banking Association should support the development of standardised questionnaires for onboarding potential VASPs, capturing key information on ownership, compliance structures and operational models.
- Secure channels should be established for intelligence exchange between financial institutions, regulators and VASPs, particularly for known exchange identifiers and suspicious wallet addresses.
- Regulators should mandate that VASPs have specific references with a VASP identifier in payment messages for bank transfers initiated on behalf of their customers, enabling the beneficiary bank to proactively identify and investigate them when needed.

Introduction

From January 2024 to September 2025, North Korea is estimated to have stolen at least $2.8-billion worth of VAs.[1] The process to subsequently launder these funds has been thoroughly documented, covering on-the-blockchain indicators related to North Korea. However, existing research only slightly touches on indicators at the point of VA-to-fiat conversion in the North Korean scheme. Gathering information on such exchanges is essential for measures to restrict the regime's access to funding its WMD programme.

VA-to-fiat currency trading services frequently appear in North Korea cybercrime investigations. Cyber actors generally attempt to cashout VAs to purchase goods and services. Importantly, North Korea is not limited to using these services for benefit. One case that falls outside of this behaviour, for example, involves North Korea using VAs to recruit a South Korean official.[2] This paper does not cover those additional channels, which merit further analysis; rather, it analyses North Korean schemes at the intersection of these blockchain-based and financial channels, to define a baseline of characteristics that could combine to form proliferation finance exposure. These features included the following indicators:

- services offered by third-party facilitators
- platforms used by facilitators
- communication trends
- proliferation finance (PF) indicators
- currency types
- locations and
- financial institution touch points.[3]

1. Multilateral Sanctions Monitoring Team (MSMT), 'The DPRK's Violation and Evasion of UN Sanctions Through Cyber and Information Technology Worker Activities', 22 October 2025, p. 25, <https://msmt.info/Publications/detail/MSMT%20Report/4221>, accessed 22 October 2025.
2. Jeong Bitna, '北해커, SNS·비트코인으로 장교 매수 … '전장망' 통째로 뚫릴뻔' ['North Korean Hackers Buy Officers via SNS and Bitcoin … The Entire "Battlefield Network" Nearly Breached'], Yonhap News Agency, 28 April 2022, <https://www.yna.co.kr/view/AKR20220428156000504>, accessed 22 April 2025.
3. Information was sanitised for this publication.

The paper first provides an overview of these indicators. It then explores risk-mitigation strategies that the private sector can implement based on these indicators. These risk-mitigation strategies apply to broader financial crime types. However, it is critical to close foundational gaps to build a more robust monitoring and detection system.

Definitions

This paper uses the FATF's definition of a VA: 'a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes'.[4]

In turn, 'facilitators' that support VA-to-fiat conversion in North Korean schemes can fall under three categories: those that are complicit in the laundering process; those that are unwittingly supporting PF activity due to deception; and those that provide liquidity to services that wittingly or unwittingly support North Korea.

The 'private sector' here refers to financial institutions, designated non-financial businesses and professions, VASPs and other commercial entities whose activities may expose them to financial crime risks or whose cooperation is necessary to prevent, detect and report illicit financial activity.

Finally, this research adopts FATF's definition of 'any natural or legal person', 'and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person': 'exchange between virtual assets and fiat currencies'; exchange between VAs; 'transfer of virtual assets'; 'safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets'; and 'participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset'.[5]

4. Financial Action Task Force (FATF), 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations', updated October 2025, <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>, accessed 27 November 2025.
5. *Ibid.*

VA-to-Fiat Conversion in North Korean Money Laundering Schemes

This chapter provides a baseline of indicators, which research conducted for this paper found to be particularly applicable to North Korea-affiliated money laundering schemes at the nexus of blockchain and financial systems.

At a granular level, North Korean threat actor groups have different techniques, tactics and procedures when moving VAs into fiat currency or cash.[6] Blockchain investigators can often distinguish each group by analysing its digital fingerprint. In some cases, this enables attribution of transactions to specific North Korean threat actors and their affiliates, such as facilitators or organised crime groups.[7] According to two interviewees, North Korean groups 'won't go too far from what they know works'.[8]

North Korea's reliance on third-party groups for the laundering process can be a challenge for the private sector when it assesses proliferation indicators. Rather than operating through isolated laundering channels, North Korea-linked funds may become intertwined with wider illicit financial ecosystems.

Hence, research for this paper seeks to determine how investigators can identify the stage in the laundering process when North Korea transfers funds to a third party. For instance, a VA investigator highlighted that a transfer from North Korean control can be inferred when funds are commingled with proceeds from activities such as 'pig butchering' scams or when they are transferred to addresses associated with entities

6. Author interview with two representatives from ZeroShadow, VA investigation company, online, 20 October 2025, <https://zeroshadow.io/>, accessed 19 November 2025. For more information on the organisation of North Korean cyber actors, see Michael Barnhart, 'Exposing DPRK's Cyber Syndicate and Hidden IT Workforce', 16 May 2025, p. 37, <https://reports.dtexsystems.com/DTEX-Exposing+DPRK+Cyber+Syndicate+and+Hidden+IT+Workforce.pdf>, accessed 22 October 2025.
7. Author interview with two representatives from ZeroShadow.
8. *Ibid.*

such as the Cambodia-based Huione Group.[9] An overview of Huione Pay, a business set up by Huione Group,[10] is provided by Elliptic in Box 1.[11]

Box 1: Elliptic Analysis: Huione Pay as a Facilitator

In July 2024, Tether froze USDT held in one of Huione's cryptocurrency wallets. This reportedly occurred after the wallet received about $35-million worth of cryptocurrency connected to the North Korea-attributed hack of the DMM cryptocurrency exchange.[12] Media coverage at the time did not differentiate between Huione Guarantee and Huione Pay, and incorrectly stated that the funds were sent to the Huione Guarantee marketplace. In reality, they were sent to Huione Pay.

Huione Pay, a payments business operated by the Huione Group conglomerate, offered a mobile application and has physical branches across Cambodia. It was widely used by Chinese nationals in Cambodia, partly as Chinese was its primary operating language. Customers could deposit cryptocurrency and exchange it for fiat currency. While both Huione Pay and Huione Guarantee were associated with Huione Group, they served different functions.

In May 2025, the Huione Guarantee marketplace was de-platformed from Telegram. Then, in December 2025, Cambodia's National Bank announced the liquidation of Huione Pay.

9. Author interview with Expert R, VA investigation company representative, online, 3 November 2025. Pig butchering is an investment scam that entails fraudsters building the trust of their victims and then deceiving them to invest in fraudulent investment opportunities. Off-ramping is the process of converting virtual asset to fiat currency.
10. Financial Crimes Enforcement Network, 'FinCEN Finds Cambodia-Based Huione Group to be of Primary Money Laundering Concern, Proposes a Rule to Combat Cyber Scams and Heists', 1 May 2025, <https://www.fincen.gov/news/news-releases/fincen-finds-cambodia-based-huione-group-be-primary-money-laundering-concern>, accessed 1 December 2025.
11. Tether is a stablecoin issuer. USDT is a stablecoin pegged to the US dollar, issued by Tether.
12. Data provided to the authors by blockchain-analytics company Elliptic, 10 November 2025, <https://www.elliptic.co/>, accessed 19 November 2025; Elliptic, 'Elliptic Data Leads to the Shutdown of the Two Largest Online Criminal Marketplaces of All Time', 14 May 2025, <https://www.elliptic.co/blog/elliptic-data-telegram-market-takedown>, accessed 10 December 2025.

In other cases, a third party may buy stolen VAs from North Korea at a discounted rate before conversion. This transfer of funds is detailed by ZeroShadow, an incident-response company, through an analysis into the Bybit laundering process. North Korea's hack of the exchange, which occurred in February 2025, resulted in it stealing almost $1.5 billion from Bybit.[13] ZeroShadow found that North Korea relied on a network of launderers, over-the-counter (OTC) traders and peer-to-peer (P2P) traders to launder and cash out funds. These facilitators were often Chinese nationals who worked around the clock to move the funds.[14] Highlighting the speed of such networks, the MSMT stated that all the funds from the Bybit hack in February 2025 were 'cashed out and converted into fiat or hard currency' as of September 2025.[15]

On-chain indicators, or actor-specific tendencies on the blockchain, also support identification of the transfer from North Korea to third-party actors. Sanitised insight in the transfer of funds between North Korea-affiliated actors and a third party is detailed by Elliptic in Box 2.

Box 2: Elliptic Analysis: Suspected Handover to Outside Launderers

Elliptic also noted that funds obtained in North Korea-attributed hacks may be transferred to third parties (including Chinese money laundering groups) during the laundering process.[16] The funds often pass through many blockchain addresses on many different blockchains while being laundered. Ownership can change at any point in that process. However, there is a belief that the change of ownership often occurs on the Bitcoin blockchain. This belief comes from analysing transaction patterns and identifying characteristics and changes in behaviour. In this case, the third-party launderers then continue the laundering.

13. Bybit, 'Bybit Security Incident: Timeline of Events and FAQs', 3 March 2025, <https://learn.bybit.com/en/this-week-in-bybit/bybit-security-incident-timeline>, accessed 10 November 2025.
14. ZeroShadow, 'North Korea Laundered $1 Billion of Crypto in 4 Months. How Industry Leaders Can Change Crypto Freezes and Recovery', 16 July 2025, <https://zeroshadow.io/blog/north-korea-laundered-usd1-billion-of-crypto-in-4-months-how-industry-leaders-can-change-crypto/>, accessed 14 November 2025.
15. MSMT, 'The DPRK's Violation and Evasion of UN Sanctions Through Cyber and Information Technology Worker Activities', p. 25.
16. Data provided to the authors by Elliptic, 10 November 2025.

In turn, the increasing overlap between North Korea-linked activity and established money laundering networks has important implications for the private sector in identifying proliferation financing exposure. VASPs, for instance, may not clearly distinguish such indicators once North Korea's proceeds enter criminal ecosystems, and PF indicators may become difficult to distinguish from indicators associated with other forms of illicit finance. The following sections outline North Korean and North Korea-linked behaviours at VASPs to aid identification of PF activity.

Communication Patterns Relevant to North Korean Activity

VASP customer service representatives should monitor for a combination of certain communication indicators that are attributable to North Korea or linked facilitators. Notably, by itself, placing pressure to unfreeze assets is not itself a primary indicator; this behaviour is normal for any type of customer. However, this activity, coupled with mule account indications, the use of specific languages, virtual private network (VPN) types, device IDs and the beneficiary address can indicate potential PF activity. Therefore, a holistic approach needs to be taken when identifying PF indicators. Below is an example provided by one interviewee for communication patterns associated with North Korea.

Box 3: Customer Service Communication Pattern

On qualitative indicators of North Korea-linked transactions, a VASP representative noted how North Korea-linked launderers interact with VASP customer service staff when they delay a transaction processing for further analysis.[17] In the past, the launderers were quieter if a VASP held a transaction. They would email, asking about what happened and if they could receive a refund. When they were told 'no', the conversation would end. How North Korea-linked individuals communicate with customer service has now changed when a VASP holds a transaction for further investigation.

According to the representative, the communication with customer service can involve 50–70 tickets submitted by the customer. Typically, the customer states they want a refund for the held funds. The money mule account may pass know-your-customer (KYC) controls for verification. The VASP will ask for the source of funds from the customer and, in return, the customer will either not respond or become rude. The customer may indicate that the source of funds is from a friend, a gift or inheritance. Instead of providing proof of the source of funds, they would continue the story that there are no checks or receipts to verify the transfer, and that the meeting was face-to-face.

When English is used for communication by North Korea-linked individuals, it is written with proper grammar and complicated English sentences, which can reflect other tools being used to generate responses.

Furthermore, the representative highlighted that North Korea-linked individuals may curse in Chinese and complain to the top management of the wallet.

In addition to interacting with customer service, North Korea-affiliated launderers are more actively posting complaints on public platforms about frozen funds. For example, interviewees from a VA investigation company noted that users complained on Telegram channels about funds being frozen with mentions of transaction hashes tied to the Bybit hack.[18]

17. Author interview with Expert C, VASP representative, 8 October 2025.
18. Author interview with two representatives from ZeroShadow.

Further, a VASP representative stated that North Korea-affiliated launderers prefer VA services that are:

- relaxed about AML compliance; and
- more likely to take the side of their customers when the customer complains about frozen transactions.

A VASP representative highlighted two platforms – whose names are withheld in this paper – that North Korea has exploited for laundering funds.[19] According to the interviewee, the platforms are likely to favour the customer's position unless there is compelling evidence that the funds originate from a hack.[20] These platforms are popular in Asia and have a good public image. However, since North Korea-linked launderers have recently become more active in complaining in public forums about funds being frozen, such criticism can impact business reputation for the platforms. These public complaints influence the reputation of the wallet providers if other customers are unaware that another customer is a North Korean actor conducting sanctions evasion.

Small Transaction Amounts

Another notable characteristic of North Korea-linked transactions when converting VA to fiat currency is the relatively small transaction amounts. A VASP representative highlighted North Korea's use of P2P marketplaces,[21] which North Korean actors can use to sell approximately $7,000 in a stablecoin, piece by piece, to individuals in return for cash or fiat currency. These thresholds could also bypass banking thresholds set for further investigation.[22] On a slightly larger scale, the breakdown into small transactions is supported by ZeroShadow's work. According to its investigations, launderers of North Korean funds split transactions 'into as little as $30K each so a freeze would not be overly impactful'.[23]

19. Author interview with Expert C, VASP representative, online, 8 October 2025. The paragraph reflects an unverified opinion expressed by the interviewee. Therefore, the platform names are withheld. The data is included to illustrate a potential exploitation gap. If North Korea is publicly posting complaints on forums with virtual asset addresses, this represents a channel for information gathering.
20. Author interview with Expert C, VASP representative, online, 8 October 2025.
21. Peer-to-peer marketplaces are platforms that enable buyers and sellers to directly transact without an intermediary.
22. Author interview with Expert L, VASP representative, online, 20 October 2025.
23. ZeroShadow, 'North Korea Laundered $1 Billion of Crypto in 4 Months'.

Money Mules

A VASP representative noted that during their internal investigations, KYC documents from North Korean actors, considered along with specific transaction patterns, tended to point to money mules. Broadly, money mules were individuals from Asia, primarily Filipinos, Indonesians or Chinese.[24] In other interviews, representatives of a VA investigation company and a VASP highlighted that their surveillance of North Korean schemes identified that the accounts are often money mules.[25] The preference for money mules from Southeast Asia is due to the low purchase cost of credentials, so a significant number can be purchased and used to set up accounts at scale.[26]

To understand North Korean operating preferences, it is important to highlight the money mule types that are available. There are many ways to recruit money mules. However, for those set up by individuals and sold online, there are two primary models for money mule accounts. Those categories are discussed in Table 1.

Table 1: Money Mule Categories

First Money Mule Model	Second Money Mule Model
An individual or entity sells credentials for payment. Following the purchase, the seller is not reachable for further communication. The data provided by the seller can include the associated email, photo and login password, which allows the buyer to change credentials. These options allow safer operational security, especially if it is a non-resident drop account.	The buyer still has access to the money mule that sold the credentials. The buyer can respond to VASP requests, complain or provide a proof-of-life update. For criminals, according to the AML compliance representative, this process includes more risk, as communication between the money mule and the buyer provides more evidence for law enforcement to track. This option is also more expensive.

Source: Author interview with Expert J, AML compliance expert, 9 October 2025.

According to the AML Compliance Specialist, the first model does not work – unless a deepfake is used for voice and video – for when a VASP requests proof of life following the identification of suspicious activity. Proof of life can involve a biometric liveness test where the customer is required to replicate gestures. Therefore, the second model for money mules is more valuable for criminals with accounts at VASPs that have reoccurring, spontaneous customer verification checks.[27]

The preferred type of money mule depends on the threat actor responsible for the money laundering procedure. For example, during the Bybit hack, TraderTraitor – a North Korean group – used Chinese organised crime groups to launder the funds and

24. Author interview with Expert C.
25. Author interview with two representatives from ZeroShadow; author interview with Expert L.
26. Author interview with Expert L.
27. Author interview with Expert J, AML compliance specialist, online, 9 October 2025.

give cash back to it.[28] Therefore, the money account preference would be those that are more commonly used by the Chinese organised crime group.[29]

For other North Korean threat actors that launder their own money, mule accounts will have probably been bought on Telegram.[30] They may recruit mules on Telegram to get accounts set up at VASPs. These recruited people are more valuable because they can do other tasks. For example, according to two interviewees, 'if we freeze an account at a particular service, the best way that DPRK [North Korea] can do something about it is to get a legitimate person to scream and shout about it. However, after explaining to the mule that the individual they are acting on behalf of represents a DPRK individual, they usually do not want to be involved'.[31]

This activity is reflected in two separate instances provided by interviewees. According to a VASP representative, 'a customer submitted a complaint about a delayed transaction via email in Korean. However, the account information showed a woman from Indonesia. Later in the conversation, the DPRK-linked actors started to use English'.[32] In a similar manner, a VA investigator noted that a separate case involved the use of an account tied to a woman in the Philippines, who passed KYC controls in return for payment from North Korean actors. The woman put pressure on the VASP to unfreeze assets on behalf of North Korea.[33] The following section provides a more detailed exploration of this practice.

Other Proliferation Finance Identifiers

According to a VASP representative, the individuals involved in North Korean laundering procedures are 'crypto natives and understand products and services that are centralized and decentralized'.[34] One notable identifier is that they use decentralised finance applications extensively, implementing mixers, bridges and self-hosted wallets to move funds and do it at scale.[35] ZeroShadow research underscores this statement by noting that 95% of North Korean stolen funds from the Bybit hack flowed through decentralised services.[36]

28. Author interview with two representatives from ZeroShadow. According to the MSMT, TraderTraitor 'originated between 2016 and 2017 when the Reconnaissance General Bureau formed a new, specialized cybercrime team tasked with stealing cryptocurrency for the DPRK'. See MSMT, 'The DPRK's Violation and Evasion of UN Sanctions Through Cyber and Information Technology Worker Activities', p. 15.
29. Author interview with two representatives from ZeroShadow.
30. *Ibid.*
31. *Ibid.*
32. Author interview with Expert C.
33. Author interview with Expert R.
34. Author interview with Expert B, VASP representative, online, 3 October 2025.
35. *Ibid.*
36. ZeroShadow, 'North Korea Laundered $1 Billion of Crypto in 4 Months'.

If a hack occurs, a crucial step for obligated entities is to have a robust incident response procedure that allows for tracing funds within 72 hours immediately after the hack. According to the interviewee, North Korea uses pre-arranged wallet structures that auto-distribute assets in real time to pre-arranged destinations, often to P2P marketplaces in South Asia or unregulated exchanges in Latin America. Such rapid, pre-arranged distribution is treated as another indicator of North Korean involvement.[37]

To support VASPs in the recognition of potential exposure, Table 2 provides an overview of methods deployed by North Korea-linked facilitators listed in the literature. Notably, these methods should not be considered as solely indicators of North Korea's involvement. For example, the methods in Table 2 can be similar to general money laundering activity.

Table 2: Table of Behaviours Used by VA-to-Fiat Facilitators in North Korean Cases Cited in the Literature[38]

Behaviours at VASPs Cited in North Korean Laundering Cases	Year of Cited Method[39]
Unregistered VASPs (including OTC traders)[40]	**2025**
Mixers[41]	**2025**
Bridges[42]	**2025**
The use of a large number of wallets in complex transaction patterns[43]	**2025**
Two or more individuals that operated through independent and linked accounts at VA exchanges[44]	**2018–19**
At one exchange, significant transfers between two individuals and third-party accounts[45]	**2018–19**
Dormant VA accounts without deposits for approximately two months prior to the hack of the exchange[46]	**2018–19**

37. Author interview with Expert L.
38. US Department of the Treasury, 'Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group', press release, 2 March 2020, <https://home.treasury.gov/news/press-releases/sm924>, accessed 22 September 2025.
39. The year of the cited method reflects one of two approaches. If the time of this specific activity is cited in the literature, this information is reflected in the table. If the activity is cited in more than one case study, the earliest date of the activity identified in the literature review of such activity occurring is depicted as the minimum threshold for the time range.
40. FATF, 'Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers', June 2025, p. 19, <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf>, accessed 22 September 2025.
41. *Ibid.*
42. *Ibid.*
43. *Ibid.*
44. US Department of Justice, 'United States of America v. Tian Yinyin and Li Jiadong', US District Court for the District of Colombia, Case 1:20-cr-00052-TJK, Document 1, filed 27 February 2020, <https://www.justice.gov/d9/press-releases/attachments/2020/03/02/yinyin_jiadong_indictment-filed_0.pdf>, accessed 22 September 2025.
45. *Ibid.*
46. *Ibid.*

Behaviours at VASPs Cited in North Korean Laundering Cases	Year of Cited Method[39]
A newly added bank account linked to a VA exchange account less than a week after the theft of funds[47]	**2018–19**
Transferred nearly $1.4-million worth of Bitcoin into prepaid Apple iTunes gift cards[48]	**2018–19**
Hundreds of automated transactions[49]	**2018**
Doctored photographs to circumvent KYC controls at VA exchanges[50]	**2018**
Falsified documentation to circumvent KYC controls at VA exchanges[51]	**2018**

In addition to these behaviours cited in the literature, Table 3 provides PF indicators cited in interviews with private sector representatives and data from Elliptic.

Table 3: Table of PF Indicators Related to Hacks Cited in Interviews

PF Indicators at VASPs Cited in Interviews
English (US) as the primary language and Korean language settings, occasionally, as a secondary language[52]
Certain VPN services (Astrill VPN, ExpressVPN, Proton VPN)[53]
Perceived automated transactions due to the number of transactions processed in a short period of time[54]

Analysis of PF Indicators in Table 3

When customers access an online platform, VASPs can monitor IP addresses. With certain tools, these providers can determine IP addresses associated with VPN services. When such tools are available, VASPs should cross-check customer IP addresses with VPNs commonly used by North Korea, such as Astrill VPN.[55] According to a 2025 report by SentinelLABS, Astrill VPN is a service 'popular among North Korean

47. *Ibid.*
48. *Ibid.*
49. US Department of Justice, 'Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency from Exchange Hack', press release, 2 March 2020, <https://www.justice.gov/archives/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack>, accessed 22 September 2025.
50. *Ibid.*
51. *Ibid.*
52. Data provided to the authors by blockchain-analytics company Elliptic, 10 November 2025, <https://www.elliptic.co/>, accessed 19 November 2025.
53. Author interview with Expert C; data provided to the authors by Elliptic.
54. *Ibid.* According to a VA investigator, this automated process can occur with bots that spread out the funds, dividing each sum of funds into 10 different addresses. However, the funds are not commingled with other sources, so it is traceable. Author interview with Expert R.
55. Author interview with Expert B; author interview with Expert R; author interview with Expert U, cybersecurity specialist, online, 10 November 2025.

threat clusters'.[56] A VA investigator emphasised this point, noting that Astrill VPN is, by default, perceived as North Korean activity; only on a few occasions is it a Chinese national.[57] However, a cybersecurity specialist highlighted that North Korean actors are aware of this Astrill VPN indicator and are shifting to new VPN services to evade detection.[58] Elliptic provided data that North Korean-affiliated entities commonly use ExpressVPN, Astrill VPN, and, more recently, Proton VPN.[59] Notably, VPN services with a large customer base, such as Proton VPN and ExpressVPN, should not be considered a clear indicator for North Korean activity but should be assessed with respect to other factors when considering PF exposure.[60] For these platforms, customers hold accounts for legitimate purposes.[61]

As an additional indicator to VPNs, identifying and tracking device IDs of customers can aid obligated entities with monitoring North Korean activity. In the case of a decentralised platform, a VASP representative highlighted that North Korea changes IP address when it performs quick swaps, but devices are changed less often. Therefore, the VASP can add certain device IDs to its blocklist and receive alerts on the devices used by a customer.[62] Furthermore, interviewees from a VA investigation company stated that there is a clear change in the device IDs identified by VASPs when North Korea is supported by third-party groups to launder funds.[63]

56. Aleksandar Milenkoski, Sreekar Madabushi and Kenneth Kinion, 'Contagious Interview | North Korean Threat Actors Reveal Plans and Ops by Abusing Cyber Intel Platforms', SentinelLABS, 4 September 2025, <https://www.sentinelone.com/labs/contagious-interview-threat-actors-scout-cyber-intel-platforms-reveal-plans-and-ops/>, accessed 8 October 2025.
57. Author interview with Expert R.
58. Author interview with Expert Y, cybersecurity specialist, online, 10 November 2025.
59. Data provided to the authors by Elliptic.
60. Author interview with Expert C.
61. Author interview with Expert R.
62. Author interview with Expert C.
63. Author interview with two representatives from ZeroShadow.

The Fiat Currency Side

Another component of the broader money laundering network that should be considered is how North Korea receives fiat currency or cash in return for VAs. Integration into the traditional financial system is outlined in this section. In Box 4, Elliptic provides insight into how North Korea has received funds by its investigation into 'guarantee marketplaces'.

Box 4: Elliptic Analysis: Guarantee Marketplaces as a Facilitator[64]

Over the past two years, there has been growing international awareness and scrutiny of illicit online marketplaces with Chinese as the primary language. These marketplaces are sometimes referred to as 'guarantee marketplaces' and exist on the Telegram messaging application. They primarily offer money laundering services, technical tools and other related services. Their general use by Southeast Asia-based transnational organised crime groups, particularly those involved in cyber scams, has been well documented.[65]

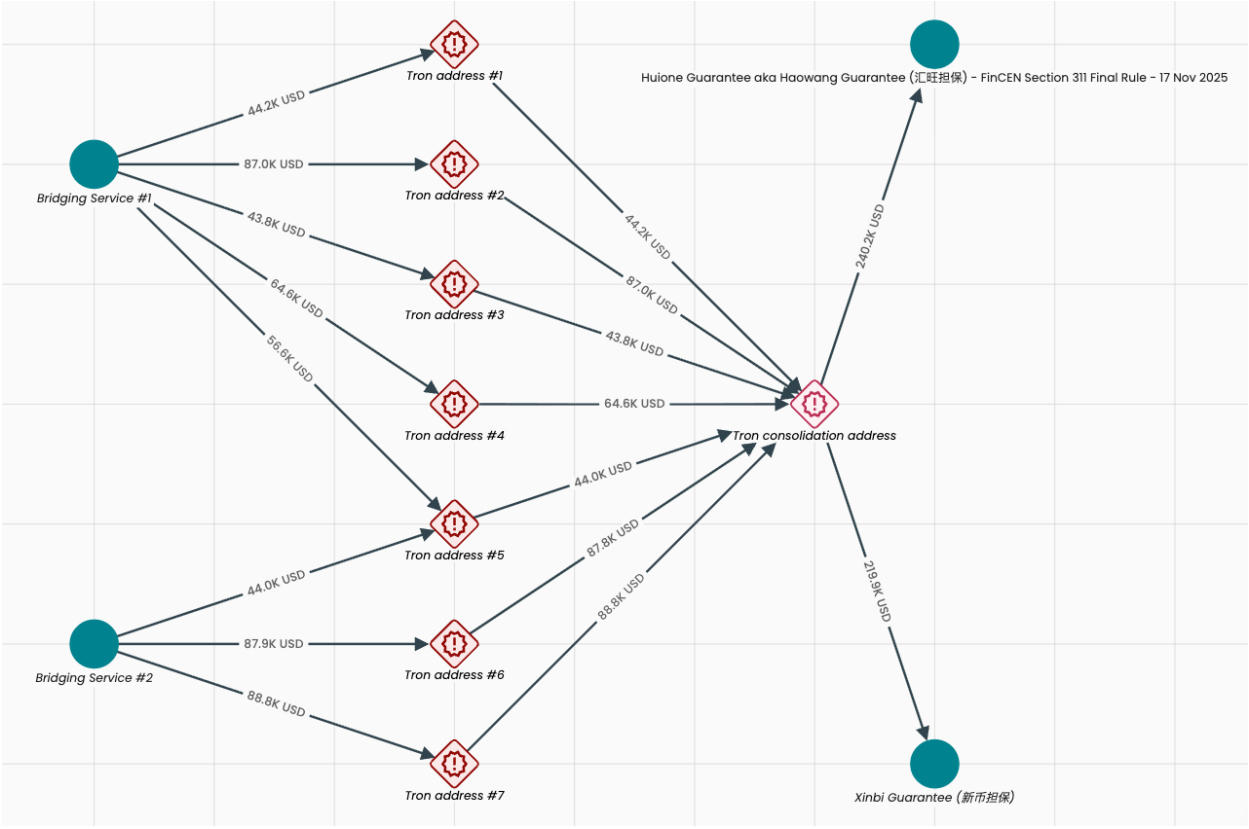
Many merchants on these marketplaces openly advertise their illicit offerings for prospective customers to see. These marketplaces also support separate private escrow deals, where staff members facilitate private deals between two parties.

Elliptic has observed instances where cryptocurrency originating from North Korea-attributed hacks has been entered into these private escrow deals. While the specific terms of these deals are unknown due to their private nature, they may involve the cryptocurrency being swapped for cash.

Figure 1 is an example observed while tracing funds linked to a North Korea-attributed hack of WazirX. Some of the stolen funds were bridged onto the Tron blockchain, consolidated and then transferred to addresses associated with private escrow services on both Xinbi Guarantee and the now-defunct Huione Guarantee.

64. Elliptic, 'Huione Guarantee: The Multi-Billion Dollar Marketplace Used by Online Scammers', 9 July 2024, <https://www.elliptic.co/blog/cyber-scam-marketplace>, accessed 10 December 2025.
65. Data provided to the authors by Elliptic, 10 November 2025. See also Elliptic, 'Xinbi: The $8 Billion Colorado-Incorporated Marketplace for Pig-Butchering Scammers and North Korean Hackers', 12 May 2025, <https://www.elliptic.co/blog/xinbi-guarantee>, accessed 10 December 2025.

Figure 1: Funds Associated with a North Korea-Attributed Hack Being Entered into Private Escrow Deals



Source: Data provided to the authors by Elliptic, 10 November 2025. See also Elliptic, 'Xinbi: The $8 Billion Colorado-Incorporated Marketplace for Pig-Butchering Scammers and North Korean Hackers'.

Funds from such services should not be automatically assumed to enter or pass through regulated financial institutions. OTC offices that support VA-to-fiat conversion services can retain cash, covering many fiat currency types. This allows for in-person cash receipt and subsequent cash smuggling, avoiding a direct deposit from a third party at a financial institution.[66] The cash, however, can be deposited at the financial institution by a courier. From a broader perspective, OTC brokers with criminal ties have used couriers to move money via ATMs, the funds from which are then taken to the financial institution by a security company.[67]

66. Author interview with Expert L.
67. Author interview with Expert N, prosecutor, online, 14 October 2025.

The MSMT reports that when 'DPRK cyber actors receive fiat currency from OTC brokers', it is 'often deposited to DPRK-controlled bank accounts through UnionPay cards issued by Chinese Banks'.[68] With this in mind, it is important for VASPs to conduct IBAN verification checks before sending funds on behalf of a customer request, including IBAN format validation and name verification.

Table 4 references the names of banks that have been reported by the MSMT in 2025 due to their use by North Korea and associated proxies in China. Tian Yinyin and Li Jiadong, facilitators that supported VA-to-fiat conversion for North Korea between December 2017 and April 2019, used eight of the banks listed in Table 4. Tian linked a bank account at China Guangfa Bank (CGB) to his VA exchange account less than a week after an exchange hack. Li, on the other hand, linked bank accounts at nine Chinese banks to his VA exchange account.[69]

Table 4: Banks Used by North Koreans and Associated Proxies in China

Name of the Bank			
Agricultural Bank of China	Industrial and Commercial Bank of China	China Merchants Bank	Zhejiang Jingning Yizuo Village Bank
China Guangfa Bank (CGB)	China Construction Bank	Bank of Jinzhou	China Zheshang Bank
China Everbright Bank	Bank of China	China Minsheng Bank	Dandong Rural Commercial Bank
Industrial Bank	Postal Savings Bank of China	Ping An Bank	China CITIC Bank
Shanghai Pudong Development Bank	Bank of Communications	Bank of Dalian	N/A

Source: The table indicates that these banks have been reported by the MSMT in 2025 for being used by the DPRK and associated proxies in China; MSMT, 'The DPRK's Violation and Evasion of UN Sanctions Through Cyber and Information Technology Worker Activities', pp. 48–49.

Obligated entities should consider this information while assessing the destination of funds and take a holistic approach in considering the information in Table 4. For example, funds moving to these financial institutions, coupled with another indicator, may result in further investigations.

68. MSMT, 'The DPRK's Violation and Evasion of UN Sanctions Through Cyber and Information Technology Worker Activities', p. 43.
69. US Department of Justice, 'United States of America v. Tian Yinyin and Li Jiadong', US District Court for the District of Colombia, Case 1:20-cr-00052-TJK, Document 1, pp. 2–3; US Department of Justice, 'Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency from Exchange Hack'.

A US indictment against three facilitators supporting North Korea with the laundering of funds alleges that they used front companies to make payments in US dollars to bank accounts owned by those listed in Table 5.[70] The payments 'were for tobacco-related products and communications equipment'. Future research should consider overlap with trade-based money laundering.

Table 5: Listed Goods Purchased by North Korean Facilitators Cited in the Literature

Bank Account Owner	Location of Company	Location of Bank	Payment Reference Field
Business involved in the procurement and/or distribution of tobacco products	UAE	UAE	Not documented
Two unidentified individuals	Not documented	Thailand	Communication device
Licensed manufacturer of tobacco products	Bulgaria	Bulgaria	Not documented

Source: US Department of the Treasury, 'Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group'.

Given that information, documentation for goods purchased by financial facilitators supporting North Korea may not appear to be high risk. VASPs that allow for business accounts should ensure that such parameters are considered in their risk assessment.

This chapter defined PF indicators that the private sector should consider when determining exposure to North Korean activity. The next chapter further defines risk-mitigation strategies that should be implemented by the private sector to further strengthen counter proliferation finance (CPF) measures. These gaps represent foundational vulnerabilities that, once resolved, can help to streamline investigations involving multiple financial crime types, including PF.

70. US Department of Justice, 'United States of America v. Sim Hyon Sop, Wu Huihui, Cheng Hung Man, and Fnu Lnu, a/k/a "Live: JammyChen0150," a/k/a "Jammy Chen"', US District Court for the District of Colombia, Case 1:23-cr-00129, Assigned Date 18 April 2023, <https://www.justice.gov/usao-dc/press-release/file/1581286/dl>, accessed 15 September 2025.

Private Sector Practices and Compliance Measures for VA-to-Fiat Conversion Services that Can Strengthen CPF

This chapter examines how financial institutions and VASPs apply practical compliance controls to detect and mitigate PF risks, with a particular focus on activity linked to North Korean networks.

Observed Private Sector Practices for Financial Institutions

Onboarding New Clients

Experts indicate that if a financial institution does not have the right onboarding questionnaire in place, it may miss VA activity.[71] This may lead to the onboarding of the customer as a 'low risk' and not having the right due diligence in place. It is imperative to develop onboarding questionnaires that account for VA-related elements, therefore enabling robust KYC to be performed.[72]

71. Author interview with Expert A; author interview with Expert I, financial institution representative, online, 2 October 2025; author interview with Expert P, AML investigation company representative, online, 27 October 2025.
72. ICAEW, 'Considerations for Auditing Cryptocurrencies', 19 September 2024, <https://www.icaew.com/-/media/corporate/files/technical/technology/know-how/considerations-for-auditing-cryptocurrencies.ashx>, accessed 12 November 2025.

To understand a potential customer's transaction history and expected activities on the account, open source research is a vital complement to typical compliance checks. Institutions review corporate websites, developer repositories, job advertisements and social media activity to verify the authenticity and the consistency of what is claimed as operations.

For example, a firm declaring itself as a software developer, but advertising blockchain engineering positions or offering wallet functionality to users may warrant further scrutiny and diligence. Open source research practices also encompass cross-referencing of the website or the email address domain, as well as exchanges' IP records for potential links to known exchanges or trading platforms.[73]

If it has been established at onboarding that the fiat source of funds and/or source of wealth is derived from VAs, the financial institution must take steps to trace and understand the VA origin. Hence, the financial institution will seek to collect information to understand the origin of the fiat funds. Such information may include:

- Documentation showing conversion of VAs to fiat:
  - Requesting exchange withdrawal receipts**,** details of the wallet addresses, wallet screenshots and transaction hashes used for conversion and blockchain analysis reports.
  - Using blockchain analytics tools to trace the VAs back to their source; identify if funds flow from high-risk sources (for example, mixers, darknet markets, sanctioned entities); and assess risk exposure based on wallet or exchange risk profiles.[74]
- Statements or confirmations from the originating VASP, which will be expected to be a licensed exchange.[75] Statements of the client's account should show how the VA was acquired (for example, bought on exchange, received from mining, staking, salary or investment returns).
- Trade history or deposit history to show fiat-to-VA purchases.
- Documentation linking fiat inflows/outflows (for example, bank transfers used to purchase VAs).

73. Author interview with Expert B.
74. Author interview with Expert P. Data pertaining to practical criteria for selecting blockchain analytics providers, as well as evaluation criteria for address attribution, including provenance, transparency and error rates, remains a point of concern raised by experts. Author interview with Expert P; author interview with Experts S and V, financial institution representatives, online, 21 November 2025.
75. Verification extends beyond licensing. Institutions should independently confirm regulatory registrations with competent authorities, evaluate public disclosures and review external communications to ensure claims are accurate. Cross-validation using blockchain analytics tools and intelligence from the financial intelligence unit – where possible – can provide further assurance of the VASP's operational legitimacy.

- Narrative or declaration from the client confirming the origin of funds.
- For corporate clients, the financial institution will also request evidence of business activity and/or financial statements to evidence the legitimacy of the funds.

However, banks face significant challenges when assessing the source of VA funds received from VASPs. The information provided is often fragmented, incomplete and inconsistent. It is shared through unsecured emails or inputted into manually prepared files, such as manipulable CSV or Excel spreadsheets that lack integrity controls or standardised formats.[76] Without harmonised, visualised reporting templates, compliance teams may struggle to integrate this data with blockchain analytics tools to verify transaction histories and risk assessments. Supervisors increasingly expect banks to demonstrate a robust understanding of how VAs were acquired and whether blockchain tracing was conducted for higher-risk cases (for example, large-value conversions, cross-border transfers or exposure to mixing services).[77]

Validation of client-submitted Excel or CSV files presents further issues, as the data can be edited or incomplete, requiring manual sampling and reconciliation against on-chain records or exchange statements. In complex cases, banks may need to calculate realised or unrealised gains from various instruments – spot, derivatives, staking or mining income – to substantiate declared wealth. Overall, the lack of standardisation, auditability and technological interoperability between VASPs and banks undermines both efficiency and regulatory assurance in VA-related due diligence.[78]

VASP Due Diligence (Counterparty VASP Checks)

Banks managing relationships with VASPs that serve as fiat on- and off-ramps face ongoing challenges in performing effective due diligence and monitoring. When reviewing incoming flows from VASP accounts, banks often find that there is limited transparency about the underlying clients behind the transactions. The data provided by VASPs may not allow name-matching or verification between the account holder at the bank and the customer at the VASP. In some cases, discrepancies arise such as mismatched names, email addresses or signatories indicating that funds may originate from third parties unknown to the bank. While banks may be inclined to trust transfers from a VASP with a strong compliance record, this reliance cannot offset concerns over the quality and depth of the VASP's customer due diligence conducted when its clients are onboarded. A risk-based approach is therefore critical, with banks

76. Author interview with Expert P.
77. US Department of the Treasury, 'Joint Statement on Crypto-Asset Risks to Banking Organizations', Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation and Office of the Comptroller of the Currency, 3 January 2023, <https://www.occ.treas.gov/news-issuances/news-releases/2023/nr-ia-2023-1a.pdf>, accessed 28 October 2025.
78. Author interview with Expert T, VA investigation company, online, 27 October 2025; author interview with Expert P.

expected to tailor their oversight depending on VASPs' jurisdictions, licensing status and compliance maturity.

When fiat funds originate from a VASP, the financial institution must:

- identify the originating VASP and verify its licensing and regulatory status;
- ensure the VASP is compliant with the FATF Travel Rule and confirm that customer and transaction data has been shared appropriately (as per the Travel Rule); and
- refuse and flag – through a suspicious transaction report (STR) – funds received from unregistered or high-risk VASPs.

Monitoring for Suspicious Activity

Increasingly, financial institutions seek to enrich their transaction monitoring frameworks with off-chain data such as payment narratives, payer and payee information, KYC records, merchant identifiers and account metadata to better identify VA-related suspicious activity. This approach aims to detect the behavioural patterns associated with illicit activities, notably money mules and unlicensed VA operators. However, current data ecosystems remain fragmented. P2P platforms, e-money institutions and VASPs often operate in silos, with limited sharing of key data points such as IBAN details. Traditional financial institutions may unknowingly process VA-linked transactions, while VASPs themselves hold datasets that vary in format and quality, complicating integration. As a result, the visibility of VA-related flows across sectors remains incomplete.

Institutions have refined their monitoring for suspicious activity[79] (MSA) to detect payment activity suggestive of VA involvement. This includes, for instance, when a company's payments consistently flow to exchange-linked IBANs or its online presence shows VA-related products. This typology supports the early identification of illicit facilitators operating under commercial cover. MSA also involves filtering keywords in transaction descriptions and counterparty analysis to identify potential links with known VASPs or VA exchanges. For example, institutions flag transactions referencing wallet identifiers, VA-related acronyms or payment purposes that indicate asset conversion. Such filters enable the identification of clients conducting VA-to-fiat activity under unrelated business categories such as 'IT services' or 'software development'. This section highlights observed practices across financial institutions.

79. For further information, see Wolfsberg Group, 'Statement on Effective Monitoring for Suspicious Activity, Part 1: Moving Beyond Automated Transaction Monitoring', 2024, <https://wolfsberg-group.org/resources/168/168>, accessed 28 October 2025; Wolfsberg Group, 'Statement on Effective Monitoring for Suspicious Activity, Part 2: Transitioning to Innovation', 2025, <https://wolfsberg-group.org/resources/innovation/202>, accessed 28 October 2025.

Ongoing controls include:

- Screening all counterparties, wallets and VASPs against sanctions lists and politically exposed person (PEP)/adverse media databases.
- Monitoring transaction patterns to identify higher-risk flows linked to exchanges, P2P platforms or blockchain gateways and any anomalies (for example, large or rapid VA-to-fiat conversions inconsistent with profile).
    - Declared VA users: Tighter monitoring thresholds; expected VASP flows allowed but reviewed for reasonableness; focus on source of VAs and jurisdictional risk.
    - Undeclared (hidden) VA users: Rules attuned to identify indicators of undisclosed activity – keyword matches, repetitive VASP-like patterns, Payment Service Providers (PSPs) operating with VAs, abnormal cash/fiat-in/out behaviour.
- Using STRs to flag and report suspicious activity to the competent FIU.

It is important to note that to monitor transaction patterns, financial institutions develop a framework of detection rules used to identify potential VA activity and associated risks within customer transactions. Table 6 documents a set of typologies, monitoring and detection indicators used to identify and assess VA-related counterparties, behaviours and transaction types for financial crime risk purposes.

Table 6: Counterparty Detection Rules

Rule	Description	Example
Counterparty Detection Rules: Known or Suspected VA-Related Entities		
Known VASP counterparties	Identify transfers to/from registered VA exchanges or brokers	N/A
Unregistered or high-risk VASPs	Cross-refer counterparty names or accounts against blacklists	Offshore exchanges, mixers or non-compliant VASPs
Merchant Category Codes (MCC)	Flag card payments with VA and other high-risk MCCs	MCC 6051 includes purchases of VAs and related digital assets, foreign currency, money orders and travellers' cheques.
VA keyword detection	Screen payment references or memos for VA-related terms	'Bitcoin', 'BTC', 'Binance', 'wallet', 'USDT', among others
Behaviour and Transaction Pattern Detection Rules: Unusual Financial Behaviour Consistent with VA Activity		
Frequent small payments to multiple exchanges	Customer layering small deposits into VA exchanges	10–20 repetitive debit or credit card payments to different VA exchanges
Round-currency transactions	Common in exchange deposits/ withdrawals	Transactions of $1,000, $5,000, $10,000, repeating patterns
High-volume P2P transfers	May indicate use of P2P VA platforms	Regular payments to individuals with references such as 'USDT', 'OTC', 'wallet'
Rapid in and out flows	Deposit, followed by an outbound transfer to a known VASP within the hour	N/A
International VA corridor flows	Cross-border transfers to and from known VA exchange hubs	Funds moving to and from jurisdictions with active exchanges (Seychelles, Hong Kong, Cayman Islands)
Source of Funds and Channel Correlation Detection Rules: Inconsistencies Between Declared Customer Profile and Actual Activity		
VA behaviour without declared VA occupation	Detects unregistered VA traders/miners	Retail customer frequently deposits funds from exchanges but no VA disclosure
Mismatch between income and activity	Detects possible laundering	Low-income customer sends large wires to VASPs
Unusual use of payment processors	VA-related PSPs or merchant acquirers	N/A
Blockchain and On-/Off-Ramp Tracing Detection Rules		
Wallet address screening	Identify if customer transfers funds to/ from known VA on-/off-ramps or wallet clusters	N/A
Address risk scoring	Blockchain analytics flag funds associated with mixers, ransomware or darknet	N/A
Conversion tracing	Identify when VAs are sold for fiat through OTC desks or P2P transfers	N/A

Source: The authors.

In addition, technical data provides an additional detection layer. Financial institutions collaborate with cybersecurity teams to analyse device fingerprints, IP addresses and login metadata associated with client banking portals. Shared infrastructure between suspected clients and known VA services can indicate concealed VASP operations. Indicators – such as whether the business operates blockchain systems, has direct technical connections to VA exchanges or uses hosting services linked to the VA sector – can help to confirm whether the customer's declared activities appear consistent.

Suspicious Business Accounts and Monitoring Processes

Systemic issues exacerbate detection and disruption. VA-origin data and KYC information provided to banks are often incomplete or inconsistent, payment names do not always match the legal name or business purpose of the VASP, and institutions maintain siloed lists of VASPs that are not useful for cross-institution monitoring. Financial institutions frequently lack access to Travel Rule metadata unless they transact directly in VAs, and monitoring systems are not always configured to ingest the kinds of fields (including virtual IBANs) that would flag suspicious VASP activity. A practical mitigation would be a regularly updated, trusted-network database of verified VASP legal names, account/IBAN details and Travel Rule identifiers that is shared across regulated entities, populated in a non-commercial, public-interest framework. That source of reconciled identity and account data would significantly improve automated detection of VA-related money-mule and unlicensed-operator patterns.

Observed Private Sector Practices for VASPs

Similar to what is observed for financial institutions, a VASP's onboarding process is critical. It involves understanding the nature of the client's business, their source of funds and source of wealth. It also requires identifying the beneficial owners of the account that is being set up. This section lists practices that can enhance detection of PF indicators.

Hop Policy

Transaction analysis involves assessing whether transaction volumes are consistent with expected customer behaviour. It does so by tracing the movement of funds across addresses and identifies any exposure to illicit services or high-risk counterparties, including the number of intermediary transfers, or 'hops', involved.

Institutions implement their own internal hop policy to determine the tracing parameters when assessing exposure to wallets or transactions linked to compromised, blacklisted or sanctioned addresses. Some VASPs have policies that set a limit for how far back in a transaction history the exchange will look for links to a sanctioned entity.

The purpose is to balance regulatory compliance and risk management, on the one hand, and operational efficiency, on the other. This ensures timely transaction monitoring without overextending analytical resources. It is important to note that there is no formal guidance from competent authorities on this matter and that a risk-based approach governs the number of hops that are investigated.

Some institutions indicate that the number of hops analysed is applied on a case-by-case basis, with the cut-off determined by the customer's business case, their source of funds and transaction types (for instance, exposure to terrorism financing or child sexual abuse material). As indicated by a VASP representative,[80] specific on-chain behaviour – such as peel chains or fee-funding[81] – will also drive the number of hops.

Other institutions indicate that for standard cases, alerts are typically configured to trigger up to five hops with the exposure level driving the next steps. For instance, beyond this threshold, enhanced due diligence is performed if contextual indicators justify deeper tracing:

- Standard Exposure: Risk based; will not seek to extend to many hops (but not fewer than five); covers most transactional relationships.
- Heightened Risk Scenarios (for example, terrorist financing, child sexual abuse material, North Korea exposure): tracing may extend to many more hops, recognising that sanctioned entities frequently use peeling chains and automated transfer services to obfuscate the flow of funds.
- Manual Review Cases: When automated monitoring detects suspicious links or unclear patterns, compliance analysts may trace transactions without a fixed limit of hops back; limits depend on the available data, typology and relevance of the intermediary wallets.

This tiered approach reflects both technical constraints (as each additional hop increases processing time and cost) and business realities, as continuous deep tracing of every transaction would be operationally prohibitive.[82] However, any confirmed link to illicit activity – such as darknet markets, ransomware proceeds, terrorism financing, child sexual abuse material or North Korea-associated funds – triggers an immediate account review and potential exit of the customer relationship. Thus, institutions' policies allow deeper tracing for particular typologies.

80. Author interview with Expert B.
81. For example, a company can decide to use its own funds to pay the gas fees for a user's transaction so that the user does not have to pay for it directly.
82. Author interview with Expert C; author interview with Expert L.

General Indicators of Suspicious Activity

As discussed in the previous chapter, VASPs establish a baseline for their customers' business profiles, thus defining what constitutes business-as-usual activity for different client categories (for example, OTC brokers, liquidity providers, payment processors or retail traders). This allows for the following controls to be performed:

- Pattern recognition: Brokers and established trading entities typically exhibit consistent, high-volume transaction patterns aligned with declared business activities.
- Account structuring review: Institutional clients often maintain multiple wallets with clear segregation. Unstructured or ad hoc wallet use may indicate personal or illicit activity conducted under a business name.
- Metadata analysis: Regularly monitoring metadata – such as fiat payment descriptions, API usage frequency, trading pairs and algorithmic trade integration – will reveal whether the account is operated manually or via automated systems.

In addition, VASPs perform transaction monitoring, ensuring that the business account activity is aligned to what was established as a baseline:

- Volume and flow patterns: Flag accounts with round-number transfers, repetitive transactions of similar US dollar value, or inconsistent volume relative to declared business size.
- Cross-account transfers: Detect intra-platform transfers between related accounts.
- Notes and references: Review payment or transaction notes for patterns such as repeated currency-pair mentions ('2 BTC at [...]') or unexplained value conversions that may disguise settlement or OTC brokerage activity.
- Linking business bank accounts to personal VA accounts, adding an unusual number of credit cards ('card loading').
- Fiat linkage: Compare VA transaction flows with corresponding fiat-in/out flows. Sudden spikes or mismatches between virtual and fiat activity warrant enhanced review.
- Using personal email addresses that contain business names (for example, 'Dave at davetrading.com').
- Sudden changes in device IDs, IP addresses or contact information.

Compliance teams typically supplement transaction monitoring with off-chain intelligence:

- Business identity verification: Confirm that the account's email domain, phone number and listed contact details correspond to a verifiable business presence (for example, corporate website, directory listing or registration database).

- Beneficial ownership and affiliations: Research directors, shareholders and associated companies to identify potential links to high-risk jurisdictions or previously sanctioned entities.
- Online footprint: Look for advertisements, broker listings or social media promotions suggesting OTC, P2P or exchange-like operations without proper licensing.
- Source of funds: Require documentation on funding origins, including proof of trading income, investor contributions or third-party payments.

The Travel Rule

The Travel Rule aims to provide visibility of counterparties. It enables risk assessments, including sanctions screening, and prevents illicit activity by requiring the exchange of originator and beneficiary information. The Travel Rule compliance workflow involves the originating VASP collecting beneficiary information, creating a Travel Rule message via commercial Travel Rule platforms, and sending this package to the beneficiary institution for verification. This pre-transaction authorisation ensures that the beneficiary reviews and confirms the customer and their willingness to receive funds before settlement is triggered. Any mismatch triggers a message back.[83]

The Travel Rule enables counterparty visibility and enables the implementation of anti-financial-crime (AFC) controls – such as sanctions screening – by requiring the exchange of originator and beneficiary information, which was previously unavailable. Typically, Travel Rule platforms[84] integrate with sanction screening providers and blockchain analytics, allowing VASPs to run sanctions checks on both their customers and counterparties. The beneficiary VASP also receives verified originator customer information to conduct its own sanctions screening.

VASPs also need to focus on counterparty due diligence. The role of Travel Rule providers often begins and ends with identifying a counterparty, leaving the ultimate accountability for the accuracy of data and additional due diligence with the VASP. In addition, some Travel Rule providers are known to provide services to VASPs that are not licensed, even in jurisdictions with established regulatory regimes; some offer services to VASPs that have faced warnings or actions from other jurisdictions.[85]

The lack of consistent counterparty VASP due diligence allows unauthorised VASPs to access the broader VA ecosystem. This creates weak links that facilitate the commingling of illicit and legitimate assets. Without clear mandates and consistent enforcement, VASPs often find it inconvenient to proactively assess the regulatory status of their counterparty VASPs. This makes them reluctant to adopt robust compliance measures and prevents the cross-fertilisation of best practice.

83. Author interview with Experts Q, VA-related company representatives, online, 29 October 2025.
84. Those are compliance technology platforms that enable VASPs to meet FATF Travel Rule requirements.
85. Author interview with a representative of VASPnet (<https://vaspnet.com/>), online, 20 November 2025.

Fiat Off-Ramp: Controls and Monitoring

Controls implemented by financial institutions when managing off-ramped funds are outlined in a preceding section. This section describes the process adopted by VASPs. Financial institutions that were interviewed in the context of this research indicate that they only approve the off-ramp of funds via the customer's personal bank account.[86] Customers can withdraw from a single, registered bank account. The bank account's beneficiary information must match the account beneficiary information registered with the VASP. Typically, the process is managed and verified by external banking partners. No credit cards or payment gateways can be used for off-ramp.

However, like other sectors, it is important to highlight that there remains considerable variation in the level of compliance across the VASP sector. Certain entities maintain strong AFC controls and collaborate proactively with authorities; others show limited or no compliance oversight. As there is no uniform compliance baseline, a case-by-case assessment of each VASP's risk profile, governance practices and thus approach to fiat off-ramping is needed.[87] This highlights the need for risk-based supervision and enforcement against VASPs that fail to implement and maintain strong AFC controls.

Hence, unsurprisingly, a financial institution representative indicated that their institution does not rely on the controls stated by VASPs for matching bank account beneficiary information with the VASP's beneficiary information. The institution's policy is to rely on its own internal controls and rules to identify any potential illicit activity, regardless of assurances from VASPs. They would still request statements and account information to conduct their own assessments. While some VASPs – for instance, those regulated under the Markets in Crypto-Assets Regulation in the EU – have controls in place for rapid movement of funds and report suspicious activity, the financial institution maintains its independent verification processes.[88]

Financial entities should consider the observed practices outlined in this chapter. These practices can close information gaps, and subsequently improve monitoring and detection for multiple financial crime types, including PF. By addressing these gaps, while accounting for the behaviours of North Korea-affiliated actors listed in Chapter 1, the private sector can further limit North Korea from benefitting from the proceeds of cybercrime.

86. Author interview with Expert L; author interview with Expert O, VASP representative, online, 24 October 2025; author interview with Expert P.
87. Author interview with Expert Z, law enforcement representative, online, 24 October 2025.
88. Author interview with a representative of VASPnet.

Conclusion and Key Recommendations

North Korea continues to exploit the VA industry to generate revenue for the regime. It now increasingly relies on established money laundering networks. To support the private sector with rethinking PF indicators, this paper provided an overview of documented behaviours of North Korea-affiliated actors at the nexus of blockchain-based and traditional financial systems, as well as risk-mitigation strategies.

The following policy-oriented recommendations aim to strengthen collaboration between national regulators and private sector actors, ensuring a consistent and risk-based approach to VA-to-fiat conversion oversight.

Recommendation 1:

Regulatory Guidance on Correspondent Relationships Between VASPs

Regulators should consider issuing clear guidance on how correspondent relationships among VASPs (that is, arrangements where one VASP provides services or access to financial infrastructure on behalf of another) are to be managed, particularly when interacting with unlicensed VASPs. Establishing consistent compliance expectations for these relationships would help to reduce the risk of misuse and exploitation.

Recommendation 2:

An International Banking Association Should Support a Standard for VA Integration into the Due Diligence Templates of Financial Institutions

An international banking association should support the development of standardised questionnaires for onboarding potential VASPs, capturing key information on ownership, compliance structures and operational models.

Recommendation 3:

Information-Sharing Protocols that Involve Verified VASPs

Countries should establish secure channels for intelligence exchange among financial institutions, regulators and VASPs, particularly for known exchange identifiers and suspicious wallet addresses.

Recommendation 4:

Requirements for Payment References for VASP Transfers to Financial Institutions

Regulators should mandate that VASPs have specific references in payment messages for bank transfers initiated on behalf of their customers, enabling the beneficiary bank to proactively identify and investigate them when needed. The payment reference could include a VASP identifier. This recommendation aims to improve the capability of financial institutions to detect a customer's VA exposure and support them with distinguishing regulated entities from unknown counterparties. Further, this indicator can be factored into institutional risk assessments, helping to refine financial institutions' capacity to monitor for facilitators.

About the Authors

Allison Owen is an independent consultant focused on the policy and security dimensions of cryptocurrency and new payment methods. She holds a Master of Arts in Non-Proliferation and Terrorism Studies from the Middlebury Institute of International Studies and a Master of Arts in International Affairs from MGIMO.

Noémi També is the Founder of Tambe Advisory, an independent financial crime consultancy specialising in AML, counter-terrorist financing, sanctions and CPF. She is an Associate Fellow at RUSI's Centre for Finance and Security and a Visiting Fellow at Hull University Business School. Drawing on experience across the public, private and academic sectors, her work focuses on financial crime risk assessments, supervisory frameworks, illicit finance typologies and the application of systems thinking to complex financial crime challenges.

195 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 195 years.

RUSI is registered as a charity in England and Wales

Charity number: 210639

VAT number: GB752275038