مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

AML/CFT/CPF Thematic Review of providers of Stored Value Facilities, Retail Payment Services and Card Schemes, and Payment Token Services

May, 2026

1. INTRODUCTION

The Central Bank of the United Arab Emirates ("CBUAE") has observed that technology-enabled payment and value transfer services are growing rapidly and becoming more complex within the UAE's financial system. In particular, Stored Value Facilities ("SVFs"), Retail Payment Service Providers ("RPSPs"), and Payment Token Service Providers ("PTSPs") now play a central role in facilitating digital payments, cross-border transactions, e-commerce, and financial inclusion initiatives across the UAE.

While these business models promote innovation and improved access to financial services, they can also create new channels and/or higher risks of Money Laundering (ML), Terrorist Financing (TF), and Proliferation Financing (PF) risks. These risk factors include, but are not limited to:

1. The provision of services through non-face-to-face onboarding channels;
2. The speed, volume, and cross-border nature of transactions;
3. Reliance on intermediaries, agents, or third-party distribution networks;
4. Exposure to virtual assets or tokenised payment instruments;
5. Potential for anonymity or reduced transparency in customer relationships.

In light of these inherent risk factors, and consistent with the UAE's risk-based approach to AML/CFT/CPF supervision, the CBUAE conducted a thematic review of these sub-sectors. The thematic review assessed how effectively the relevant Licensed Financial Institutions (LFIs) in each sub-sector have designed and put into operation their AML/CFT/CPF control frameworks. The review aimed to determine whether these institutions appropriately identify and assess ML/TF/PF risks in line with their regulatory obligations, and whether they have implemented adequate controls to mitigate these risks. The themes from the review are highlighted in this report.

The review takes into consideration the relatively early stage of these institutions in business – having operated for less than five years - and evaluates the maturity of their AML/CFT/CPF frameworks within this context. The outcomes of this review will inform the CBUAE's future supervisory engagement, risk mitigation strategies, and potential regulatory or enforcement measures, where required, to ensure that innovation within the payment services sector is supported by robust safeguards against financial crime risks.

Further detail on ML/TF/PF typologies and red flags specific to SVFs and RPSCS is provided in Annex 1.

1.1. Terms and Definitions

Terms & Definitions	Description
CBUAE	Central Bank of the UAE
AML/CFT/CPF	Anti-Money Laundering, Combating the Financing of Terrorism and Counter-Proliferation Financing
AMLD	AML/CFT Supervision Department
ML/TF/PF	Money Laundering, Terrorism Financing and Proliferation Financing
RBA	Risk Based Approach
NRA	National Risk Assessment
FIU	Financial Intelligence Unit of the UAE
FATF	Financial Action Task Force
PTSPs	Payment Token Service Providers
SVFs	Stored Value Facilities
RPSCS	Retail Payment Services and Card Schemes
RPSP	Retail Payment Service Providers
LFIs	Licensed Financial Institutions

1.2. Legal Basis

As part of national efforts to combat money laundering, terrorist financing and proliferation financing, the UAE has strengthened its AML/CFT/CPF regime through the issuance of Federal Decree by Law No. 10 of 2025[1] (AML/CFT Law) and Cabinet Resolution No. 134 of 2025[2] (AML/CFT Decision), which now explicitly covers proliferation financing and digital systems, including virtual assets. Among other provisions, the AML/CFT Law and AML/CFT Decision reduces the thresholds for liability regarding compliance with AML/CFT/CPF requirements, introduces stricter penalties, and grant broader supervisory powers to the CBUAE and law enforcement agencies.

The CBUAE issued the Stored Value Facilities (SVF) Regulation in November 2020. This regulation permits a wider range of entities to apply for an SVF license and provide stored value services in the UAE. It also introduced updated measures for supervising and enforcing requirements on SVF providers operating in the UAE, except those in Financial Free Zones. The regulation requires SVF providers to comply with all applicable AML/CFT/CPF obligations, including conducting risk-based assessments and reporting suspicious transactions to the UAE Financial Intelligence Unit (FIU).

The CBUAE issued the Retail Payment Services and Card Schemes (RPSCS) Regulation in July 2021. This regulation established the licensing and supervisory framework for providing retail payment services in the UAE across nine categories, including Payment Account Issuance Services, Payment Instrument Issuance Services, Merchant Acquiring Services, Payment Aggregation Services, Domestic and Cross border Fund Transfer Services, Payment Token Services, Payment Initiation Services and Payment Account Information Services. The regulation requires licensed Payment Service Providers to implement effective AML/CFT/CPF controls to manage money laundering, terrorist financing, and proliferation financing (ML/TF/PF) risks, and to report suspicious activities and transactions to the UAE Financial Intelligence Unit (FIU).

The CBUAE issued the Payment Token Services (PTS) Regulation in June 2024. The PTS regulation provides for the licensing and registration of entities providing payment token issuance, conversion, custody or transfer services. Payment Tokens are a category of virtual assets (VAs) designed to maintain a stable value relative to fiat currency. While Payment Tokens may serve as a medium of exchange, unit of account, or store of value, they are not recognized as legal tender. Licensed Payment Token Service Providers are required to comply with all applicable AML/CFT/CPF obligations and report suspicious transactions to the FIU.

1.3. Applicable AML/CFT/CPF Laws

a. Federal Decree-Law No. (6) of 2025, Regarding the Central Bank, Regulation of Financial Institutions and Activities, and Insurance Business;

b. Federal Decree by Law No. 10 of 2025 on Combating Money Laundering, the Financing of Terrorism, and the Financing of Arms Proliferation (AML/CFT Law);

c. Cabinet Resolution No. (134) of 2025, Regarding the Executive Regulations of Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing (AML/CFT Decision);

d. Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council (UNSC) Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution (“Cabinet Decision 74”), and its amendments;

e. Cabinet Decision No. (58) of 2020 regulating the Beneficial Owner Procedures (“Cabinet Decision 58”);

2. GROWTH OF THE SECTOR (2021 to 2025)

[1] Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing

[2] Cabinet Resolution No. (134) of 2025 Regarding the Executive Regulations of Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing.

Over the past five (5) years, the following Payment Service Providers were licensed and permitted by the CBUAE to conduct payment services activities in the UAE.

	2021	2022	2023	2024	2025
SVFs	2	3	6	12	16
RPSPs	0	3	12	23	30[3]
PTSP	0	0	0	1	1

In the UAE, the payment services market is expanding significantly, driven by digital wallets, prepaid cards, and online payment platforms. As of 2025, SVFs and RPSPs made up 97.8% of all licensed financial institutions among the sub-sectors covered in this review, placing them at the centre of the payment service market's transformation. Additionally, the sector witnessed exponential growth of 195% in its customer base between the years 2023 and 2024.

The Payment Token Services sector is still relatively small, given that the payment token services regulatory regime was implemented in 2024. The sector is however expected to grow over the coming years.

In light of the growth of the sector, the CBUAE provides enhanced, risk-based supervision to the sub-sectors above, reinforcing AML/CFT/CPF compliance through onsite inspections, offsite reviews, tailored workshops and outreach programmes.

3. AML/CFT/CPF REVIEWS OF LICENCING APPLICATIONS AND SUPERVISORY ENGAGEMENTS

3.1. Licensing Applications

As an integral component of the licensing process, all applicants are subject to a comprehensive assessment of their compliance with applicable AML/CFT/CPF requirements.

As part of this process, the CBUAE evaluates the applicant's proposed business model, product offerings, delivery channels, and customer segments, with a particular focus on identifying the inherent ML/TF/PF risks associated with their intended activities. In addition, the CBUAE assesses the design and adequacy of the applicant's AML/CFT/CPF governance, risk management, and internal control frameworks at the point of the licensing application to determine whether these are proportionate to the nature, scale, and complexity of the proposed operations.

3.2. AML/CFT/CPF Supervisory Intervention

Over the past five years, following the issuance of licenses and the commencement of operations by SVFs, RPSPs, and PTSPs, a series of targeted AML/CFT/CPF supervisory interventions have been implemented. These interventions were designed to ensure compliance with AML/CFT/CPF regulatory standards and to strengthen the entities' risk management frameworks. The supervisory activities focused on mitigating inherent risks associated with the early operational stages of these entities, thereby promoting a robust and sustainable compliance culture within the payment services sector. The table below provides a summary of the CBUAE's AML/CFT/CPF supervisory interventions of the sector.

Sub-sector	**AML/CFT/CPF supervisory interventions**			
	Self-Assessments	**Full scope inspections**	**Targeted inspections**	**Outreaches; One-on-one sessions MLRO/Senior Management**
	2024 and 2025: Self-assessment	**2023, 2024, and 2025**: The CBUAE	**2024**: The CBUAE placed institutions	

[3] As of May 2026, Licensed Financial Institutions holding both SVF and RPSCS licenses are 13.

SVFs	questionnaire was used to collect and assess the AML/CFP/CTF inherent risk and controls effectiveness.	conducted onsite examinations on high-risk entities.	identified with significantly high or high risk findings on its Enhanced Monitoring Program (EMP) to ensure more intensive supervisory oversight.	• **2024 & 2025**: The CBUAE conducted sector specific outreach programmes. • **2021, 2022, 2023, 2024 and 2025**: The CBUAE conducted outreach programmes for the sectors, including for SVFs and RPSCS. • **2025**: The CBUAE conducted a Data Validation Outreach session for all SVFs and RPSCS.
RPSCS				
PTSPs		**2025:** The CBUAE conducted full scope examination prior to licensing and commencement of operations.		**2025:** The sub-sector attended the outreach program conducted by the CBUAE for all LFIs.

The payment services sector in the UAE is still in its early stages, with SVFs, RPSPs, and PTSPs all operating for less than five years. In this context, the ongoing implementation of risk-based supervisory interventions will continue to play an important role in strengthening the sector's AML/CFT/CPF controls. These interventions, which are conducted on an ongoing basis, have contributed to the progressive enhancement of the adequacy and effectiveness of the entities' AML/CFT/CPF frameworks. Continuous supervisory engagement will foster a more resilient and compliant ecosystem within the payment services sector.

4. SCOPE

To assess the effectiveness of the AML/CFT/CPF controls across SVFs, RPSCS, and PTSPs, this thematic review draws on two key supervisory data sources that provide insight into both inherent and residual risk exposures:

- Preliminary findings - licensing reviews/outcomes, and
- Sector-wide Self Assessments

4.1. Preliminary findings - licensing reviews / outcomes.

Preliminary findings during the pre-licensing process offer an early assessment of the sector's control maturity by identifying structural AML/CFT/CPF design weaknesses, governance gaps, and risk-mitigation deficiencies. These findings highlight the adequacy of initial risk assessments and the robustness of controls prior to market entry. For SVF, RPSP and PTSP applications, several key AML/CFT/CPF controls are assessed to determine design effectiveness. These include, fit and proper testing of key individuals; governance and oversight; policies and procedures; preliminary business risk assessments; customer onboarding and due diligence controls; transaction monitoring systems; sanctions screening systems; compliance function; and record-keeping and data governance practices.

If an applicant's controls do not meet the minimum AML/CFT/CPF standards, a license will not be granted. However, if the applicant meets the minimum standards but still has areas that need improvement, a license may be issued with certain restrictions, conditions, or additional requirements. In such cases, the applicant must also follow CBUAE issued risk mitigation plans.
The supervisory data gathered for preliminary findings are focused on applicants that meet the minimum standards but still have areas that require improvement.

4.2. Sector-wide Self-Assessments.

In December 2024, the CBUAE mandated all SVFs and RPSPs to complete an AML/CFT/CPF Risk Assessment Questionnaire through Notice No. CBUAE/FCS/2024/5966. A total of 26 out of the 35 SVFs and RPSPs submitted responses, which were analysed during the thematic review. An overview of the sectors' size, nature, and complexity includes the following key points:

- Number of customers: Over 1.12 million;
- Geographic reach: Business conducted across 238 jurisdictions;
- Products: Aggregate number of products offered by the SVFs and RPSPs – 96 products
- Number of Merchants: Over 92,000.

The results of the sector-wide self-assessment exercise were used to validate how well licensed financial institutions have put their AML/CFT/CPF frameworks into practice. The self-assessment results enabled comparative analysis of control effectiveness, detection capabilities, governance practices, and adherence to risk-based approaches across the sector. This analysis supported in the identification of common themes and emerging ML/TF/PF risk patterns.

Inherent risk assessment: Each entity completed ninety-four (94) structured risk questions designed to capture quantitative data points for determining its inherent ML/TF risk exposure. The data collected covered key risk factors, including customer risk, geographic exposure, products, services and transactional activity, and delivery channels.

Control effectiveness: Each entity provided responses to ninety-two (92) control-related questions. Data collected was used to determine the adequacy and effectiveness of the AML/CFT/CPF frameworks. Controls assessed included - Governance and Management Oversight; Policies and Procedures; Customer Due Diligence; Sanctions Compliance Program; Transaction Monitoring Controls; Reporting Obligations - STR or SAR identification and reporting requirements; AML/CFT/CPF Training; and Record Retention.

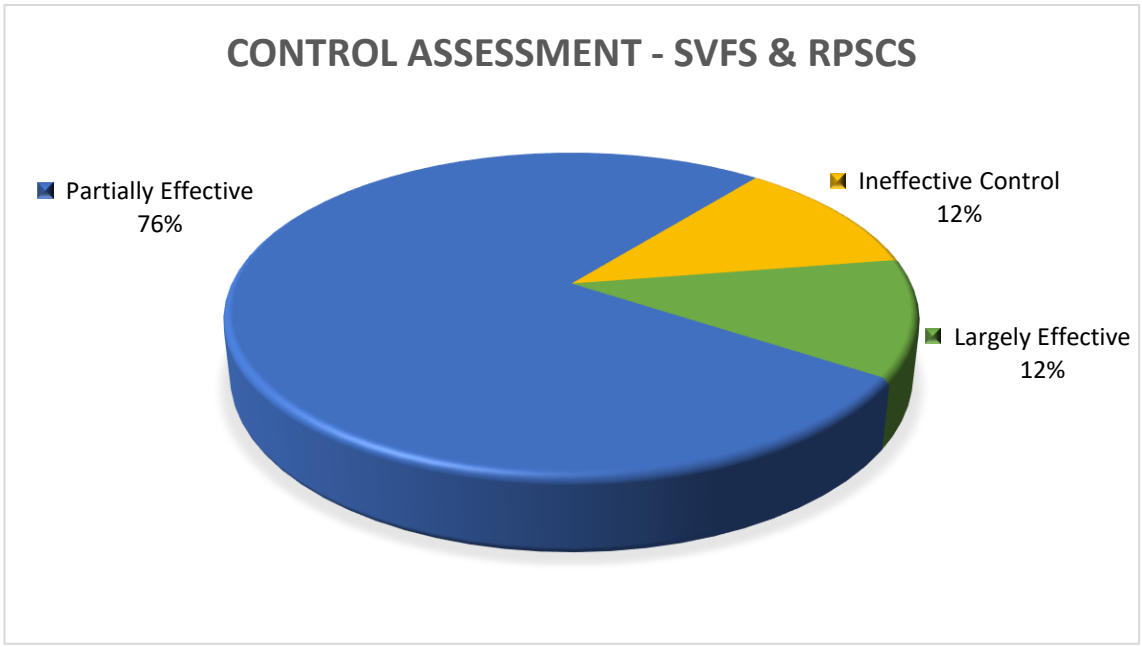
5. OVERALL OUTCOMES

This thematic review outlines the results of the assessment of the adequacy and effectiveness of the AML/CFT/CPF controls of SVFs, RPSPs and PTSPs.

SVFs and RPSPs

Data relating to key AML/CFT/CPF control factors, including the availability and adequacy of policies and procedures, transaction monitoring systems, sanctions screening frameworks, and suspicious transaction reporting mechanisms, was obtained and analysed to assess both the design and operational effectiveness of AML/CFT/CPF controls implemented by SVFs and RPSPs.

The outcomes of the controls assessment across the entities reviewed indicates that twelve percent (12%) demonstrated largely effective AML/CFT/CPF control frameworks, seventy-six percent (76%) exhibited partially effective controls. The remaining twelve percent (12%) were assessed as having ineffective controls or not yet fully established controls. In these cases, the entities were newly licensed and still in the process of finalizing their control frameworks before starting full business operations. Licenses are granted with the clear expectation that all entities will have adequate controls fully operational prior to commencing their activities. Where appropriate, restrictions are placed on institutions prior to commencing operations, and ongoing supervision is conducted to ensure that these standards are met.



Whilst SVFs and RPSPs are making tangible efforts to enhance the effectiveness of their AML/CFT/CPF framework, taking into consideration, the nature, size and complexity of their business, the Thematic Review identified specific areas where improvements can be made to strengthen compliance. To support continued progress and ensure robust controls, risk-based targeted and full-scope onsite examinations will be conducted, with higher-risk entities receiving priority attention.

PTSPs

As part of its supervisory mandate, the CBUAE conducts onsite inspections of licensed PTSPs during both the pre-licensing application process and post-licensing review phases. These examinations rigorously assess the adequacy of the PTSP's AML/CFT/CPF framework. Based on these reviews, the CBUAE identified a number of areas where PTSPs are expected to further strengthen their AML/CFT/CPF compliance frameworks. While the results of these reviews demonstrate that a positive foundation has been established, the CBUAE expects continued enhancement of controls to ensure greater resilience and alignment with AML/CFT/CPF standards and emerging sectoral risks. The review sets out a number of key areas for improvement, including:

- Improving the depth of business-wide risk assessments to better capture the nature and complexity of institutions' activities.
- Enhancing the independence of AML/CFT/CPF compliance functions, reducing reliance on parent-company resources.
- Enhancing governance arrangements, policies, and procedures to support more consistent and robust AML/CFT/CPF risk management.
- Expanding technological capabilities, particularly in blockchain analytics and travel rule compliance, to improve monitoring and analysis of on-chain and off-chain transactions.
- Applying a more risk-sensitive approach to agent due diligence to better differentiate higher-risk relationships.

6. THEMATIC REVIEW FINDINGS

6.1. STORED VALUE FACILITIES (SVFS) AND RETAIL PAYMENTS SERVICE PROVIDERS (RPSPs)

6.1.1. Governance, Management Oversight and Risk Assessments.

REGULATORY EXPECTATION.

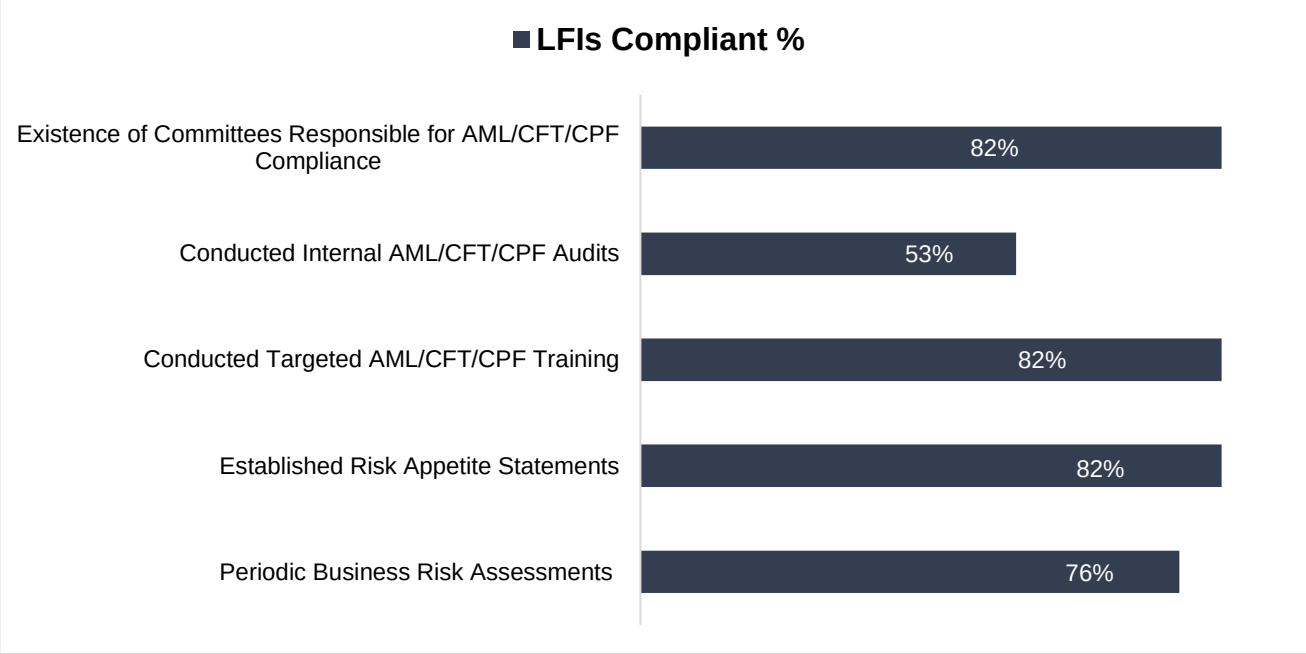
Article (19) of Federal Decree by Law No. 10 of 2025, Articles (5), (21) and (22) of Cabinet Resolution No. (134) of 2025, Article 14 of the SVF Regulation; Article 10 and 12 of RPSCS Regulation; and Section 5, Section 7 and Section 8 of CB Notice No. 3090/2021 (as amended by CB Notice No. 3599/2023), Regarding AML/CFT/CPF Guidelines for Financial Institutions, outlines the following governance management oversight expectations:

1. Senior management should set out ML/TF/PF risk appetite and a proper "tone at the top".
2. Senior management of all SVFs and RPSPs are responsible for performing certain functions related to the assessment, management and mitigation of the ML/TF/PF risks to which their organisations are exposed.
3. SVFs and RPSPs are required to appoint a qualified compliance officer in line with the requirements of the relevant Supervisory Authority;
4. SVFs and RPSPs are required to implement internal policies, controls and procedures that enable them to manage and mitigate the ML/TF/PF risks they have identified in their ML/TF/PF business risk assessment, in keeping with the nature and size of their businesses.
5. SVFs and RPSPs are required to put in place comprehensive AML/CFT/CPF policies and procedures in accordance with the AML/CFT law and regulations
6. SVFs and RPSPs should formulate and implement appropriate policies, procedures and controls with regard to staff training.

An effective AML/CFT/CPF framework is underpinned by a sound governance structure and a strong compliance culture. Accordingly, SVFs and RPSPs are required to implement effective management arrangements that establish clear accountability for identifying, managing and mitigating ML/TF/PF risks. These arrangements must be supported by appropriately resourced and independent compliance functions. The CBUAE's assessment of governance and management oversight across SVFs and RPSPs indicates a generally positive level of institutional maturity within the sector. In particular:

1. A majority of entities (76%) demonstrated the implementation of periodic Business Risk Assessments using structured and comprehensive methodologies, reflecting an increasing recognition of the importance of risk-based decision-making aligned with the size, complexity, and nature of their operations.
2. Most entities (82%) had established Risk Appetite Statements, providing a defined framework to guide risk-taking activities and support the monitoring of financial crime risks against established thresholds
3. Similarly, 82% of SVFs and RPSPs conducted targeted AML/CFT/CPF training for relevant staff, contributing to enhanced awareness of financial crime risks and regulatory obligations across operational functions.
4. Over half of the reviewed entities (53%) had undertaken internal audits of their AML/CFT/CPF programmes, indicating a growing emphasis on independent assurance and ongoing effectiveness of control frameworks.

These observations indicate that most SVFs and RPSPs have made significant progress in embedding strong governance arrangements that support the implementation of proportionate AML/CFT/CPF controls. Continued improvement is expected as the compliance frameworks of recently licensed or newly operational entities mature further.



While certain governance and organisational deficiencies were observed across the Licensed Financial Institutions, resulting in relatively higher occurrence rates, it is worth noting that these findings should be considered within the broader context of institutional maturity and proportional implementation of regulatory requirements.

In particular, a number of the SVFs and RPSPs assessed were recently licensed or are in the process of operationalising their AML/CFT/CPF frameworks. As such, the findings noted in areas relating to governance arrangements, independent assurance mechanisms, and procedural documentation may reflect transitional gaps associated with the establishment and embedding of newly developed compliance structures.

For example, a relatively small proportion of SVFs and RPSPs were observed not to have formally defined their risk assessment methodologies (24%), established dedicated committees responsible for AML/CFT/CPF compliance (18%), or implemented formal Risk Appetite Statements tailored to their business (18%).

Continued development and formalisation of governance structures and risk appetite frameworks are expected as these Licensed Financial Institutions accumulate sufficient operational data and further mature their AML/CFT/CPF control environments.

Overall, it is encouraging to note that SVFs and RPSPs have begun to establish remediation plans, further developing their foundational risk management processes. Ongoing progress is anticipated as these institutions increase their compliance resources, enhance oversight arrangements, and further develop their AML/CFT/CPF frameworks to ensure alignment with regulatory requirements.

6.1.2. Sanctions Compliance Program

REGULATORY EXPECTATION.

Article (19) of Federal Decree by Law No. 10 of 2025, Article (21, 22 and 23) of Cabinet Resolution No. (134) of 2025, Article (44, 45, 46, 47 and 48) of Cabinet Resolution No. (74) of 2020, Article 14 of SVF Regulation; Article 10 of RPSCS Regulation; Cabinet Resolution No. 50 for 2020; CB Notice No. 4368/2021, Regarding, Guidance for Licensed Institutions on Transaction Monitoring (TM) and Sanctions Screening (SS) under Section 3.7; and Section 21.2 of CB Notice No. 3090/2021 (as amended by CB Notice No. 3599/2023), Regarding, AML/CFT/CPF Guidelines for Financial Institutions outlines the following expectations for SVFs and RPSPs:

1. Sanctions Screening lists must include all names on lists issued by the United Nations Security Council (UNSC) and its relevant Committees (referred to as the "United Nations Consolidated List") and by the UAE Cabinet (Local Terrorist List).
2. On a periodic basis and in the event of material irregularities in system output, SVFs and RPSPs are required to reassess the functionality of Sanctions Screening systems and processes, including threshold settings, screening rules, and the accuracy and completeness of data used in the screening process.
3. Adequate processes must be put in place to ensure that customer and transactional data feeding into their Sanctions Screening System meets the established data quality standards, and that the data is subject to testing and validation at risk-based intervals.

To ensure effective implementation of counter financing of terrorism (CFT) controls, SVFs and RPSPs are required to have a comprehensive Sanctions Compliance Program (SCP) that clearly outlines the key eight components of the program, and provides practical guidance to employees in implementing CFT measures. The SCP should clearly include the following components: senior management commitment, risk assessment, sanctions risk appetite, internal controls, policies and procedures, training, independent audit and testing of processes and systems, and record keeping.

A significant number of the SVFs and RPSPs demonstrated strong compliance with the Sanctions Compliance Program. However, areas for improvement remain, as some deficiencies were identified in certain institutions. A summary of the observations include:

a) A significant proportion of SVFs and RPSPs (65%) have implemented comprehensive sanction screening policies, procedures and processes on transaction parties, demonstrating ongoing progress towards effective compliance. Efforts are underway for the remaining entities to achieve comprehensive alignment with these requirements.
b) The majority of SVFs and RPSPs (80%) were observed to conduct customer database screening within 24 hours of updates to the UNSC and UAE Local Terrorist Lists, reflecting a strong commitment to timely and responsive compliance measures.
c) Eighty-two percent (82%) of SVFs and RPSPs have adopted real-time sanctions screening of transactions prior to processing, highlighting a proactive approach to risk mitigation. The remaining entities had manual processes and were encouraged to further enhance their controls to achieve full compliance with regulatory expectations.
d) Opportunities exist to strengthen internal controls, as maintaining an internal watchlist for previously detected and reported cases will further enhance ongoing monitoring and risk management frameworks.
e) While some SVFs and RPSPs have initiated measures to screen trade-based transactions against the dual-use goods list provided by the Executive Office for Control and Non-Proliferation, there is continued scope for improvement.

While certain sanctions screening-related control deficiencies were observed across SVFs and RPSPs, these findings should be viewed within the broader context of operational maturity and the evolving nature of implementation of Targeted Financial Sanctions (TFS) obligations.

In particular, while some SVFs and RPSPs had initiated measures to screen trade-based transactions against dual-use goods lists issued by the Executive Office for Control and Non-Proliferation (EOCN), other entities are less vulnerable to these risks, and consequently have developed less mature controls for dual-use goods screening. This is because SVFs and RPSPs are generally not exposed to traditional trade-based money laundering (TBML) risks associated with trade finance, due to the absence of documentary trade financing

functions. Nonetheless, they may face indirect sanctions or PF exposure through payment settlement channels, warranting proportionate screening and monitoring controls. Furthermore, as the design of proportionate TBML monitoring controls are requested during the pre-licensing stage, the remaining licensed financial institutions are currently in the process of formalising system capabilities and procedural frameworks.

Similarly, gaps were identified in areas such as screening of directors of corporate customers, agents acting on behalf of customers, and ultimate beneficial owners, as well as in the periodic testing and validation of sanctions screening systems. These gaps indicate transitional challenges associated with embedding enterprise-wide screening coverage across customers, related parties and transactional data points. Challenges in periodic testing and validation are, in part, due to the limited availability of operational data required to calibrate screening scenarios and conduct effectiveness testing in the early stages of business operations.

Nevertheless, a number of SVFs and RPSPs have begun to enhance their sanctions screening controls, with continued progress expected as governance arrangements are strengthened, system integrations are enhanced, and internal assurance mechanisms are further developed in line with applicable TFS obligations.

As part of the CBUAE's risk mitigation plan, SVFs and RPSPs with weaker TBML controls were given timelines to enhance their Sanctions Compliance Programs. SVFs and RPSPs are reminded of the need to periodically review their policies and procedures, in a timely manner, and in response to events or emerging risks. Furthermore, adequate sanction screening system validation activities should be periodically conducted, and identified issues clearly presented to senior management for prompt action to address the identified issues.

6.1.3. Transaction Monitoring Controls.

REGULATORY EXPECTATION.

In line with Article (19) of Federal Decree by Law No. 10 of 2025, Article (5, 17, 18 and 22) of Cabinet Resolution No. (134) of 2025, Article (14) of SVF Regulation; Article (12) of RPSCS Regulation; and Section 2 of CB Notice No. 4368/2021, Regarding, Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening; SVFs and RPSPs are required to have an effective transaction monitoring (TM) program that enables the detection, investigation, and reporting of suspicious transactions, in compliance with the UAE's legal and regulatory framework, and ensures that customers and transactions remain within their risk appetite.

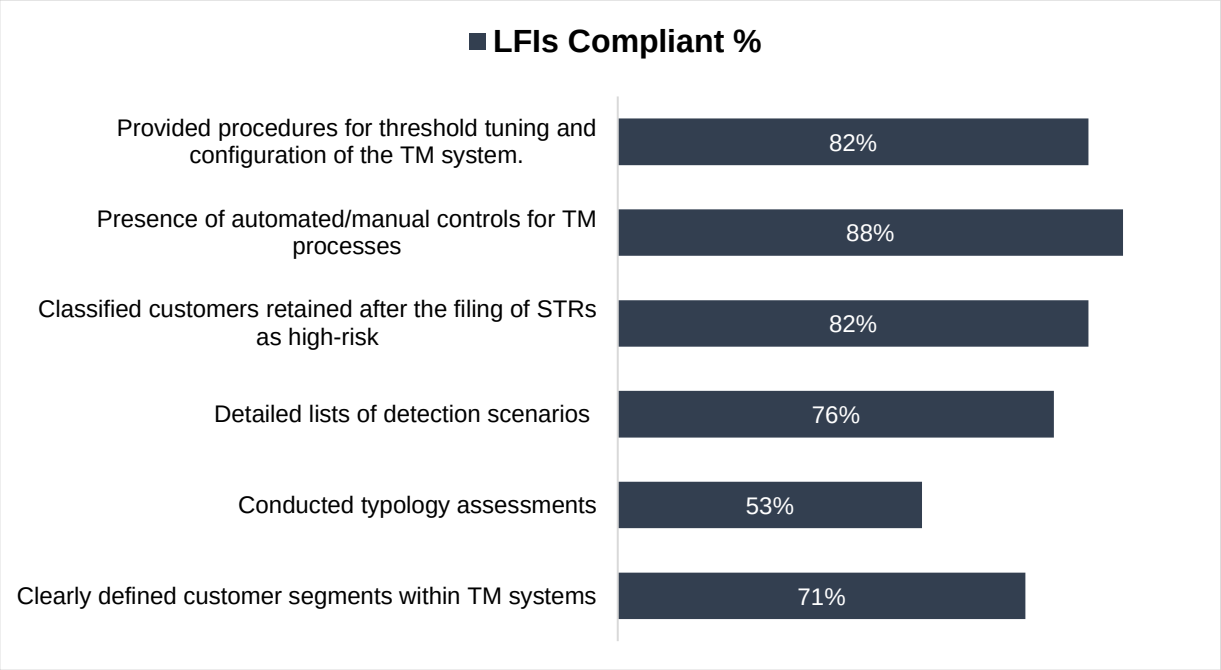
Transaction Monitoring (TM) controls are a fundamental component of the AML/CFT/CPF compliance framework applicable to SVFs and RPSPs, enabling the ongoing assessment of customer activity and timely identification of unusual or suspicious transactional behaviour. SVFs and RPSPs are required to implement automated TM systems capable of detecting potentially suspicious patterns and facilitating appropriate investigation and reporting.

This is particularly important given the inherent risks associated with their business models, which facilitate high-volume, low-value transactions through digital wallets, prepaid instruments, and peer-to-peer payment functionalities, often supported by simplified or non-face-to-face onboarding. Such features increase exposure to risks, including structuring, third-party funding, money mule activity, and the rapid placement and layering of illicit proceeds. In the absence of effective TM controls, these platforms may be misused for the movement of illicit proceeds or unlicensed remittance activity, enabling illegitimate funds to transit via the SVF and RPSP ecosystems and enter the regulated financial system through linked bank withdrawals or merchant settlement channels.

The assessment identified the following compliance outcomes for SVFs and RPSPs:

a) A substantial proportion of entities (71%) had clearly defined customer segments within their transaction monitoring systems, demonstrating a structured approach to risk differentiation and tailored controls.
b) More than half of the SVFs and RPSPs (53%) have conducted typology assessments, using these insights to inform the configuration of transaction monitoring scenarios and rules.
c) The majority of entities (76%) provided detailed lists of detection scenarios incorporated into their transaction monitoring systems during the review period.
d) Eighty-two percent (82%) of SVFs and RPSPs classified customers or business relationships retained after the filing of Suspicious Transaction Reports (STRs) as high-risk.

e) While many entities had established controls for managing multiple cards and linked accounts, there remained opportunities to further strengthen these measures, particularly where anonymous linked cards are involved.
f) A significant number of SVFs and RPSPs maintained effective monitoring of payment activities in high-risk areas. However, others lacked a sufficiently tailored approach to these specific risks.



Based on the findings presented, SVFs and RPSPs have demonstrated measurable progress in establishing foundational Transaction Monitoring (TM) frameworks across the sector, with the majority of entities having implemented automated monitoring capabilities to support the identification and reporting of suspicious activity. Only 12% had not embedded automated transaction monitoring tools, as they still are in early stages of their establishment. The observed gaps in the areas relating to typology assessments, scenario deployment, customer segmentation, and threshold tuning, reflect areas of system optimisation rather than the absence of core TM infrastructure.

Importantly, these findings indicate that SVFs and RPSPs are operating with baseline TM controls and are transitioning towards more mature, risk-sensitive monitoring environments. Enhancements in areas such as typology-driven scenario development, post-STR customer risk classification, and documentation of threshold calibration are expected to further strengthen the effectiveness of ongoing monitoring processes.

Given the high-volume, fast-paced transactional nature of the sector, continued refinement of TM systems will enable institutions to more effectively detect behavioural anomalies, including structuring, mule activity, and rapid value transfers across wallets.

Overall, the sector demonstrates a positive trajectory towards improving the sophistication of its TM capabilities in line with its evolving ML/TF/PF risk exposure and regulatory expectations.

6.1.4. Customer Due Diligence

REGULATORY EXPECTATION.

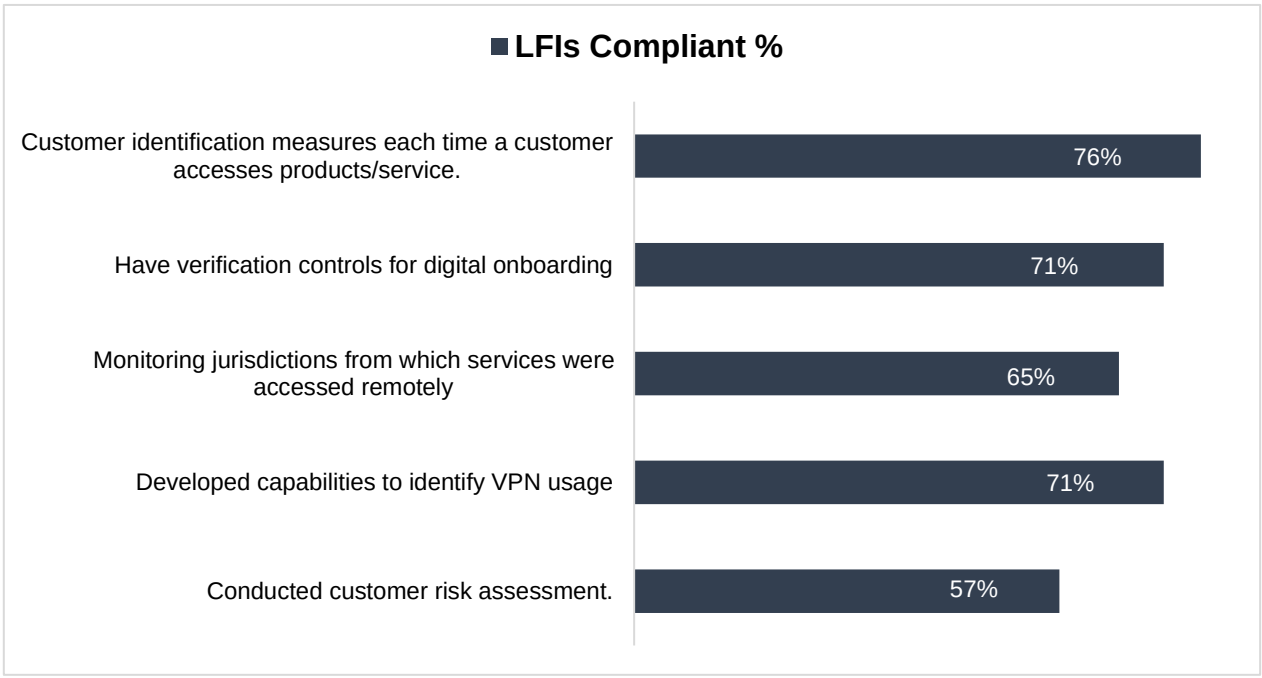
Article (19) of Federal Decree by Law No. 10 of 2025, Article (5, 6, 7, 8 and 9) of Cabinet Resolution No. (134) of 2025; Article 14 of SVF Regulation; Article 12 of RPSCS Regulation; Section 3 of CB Notice No. 4640/2022, Regarding, Digital Identification for Customer Due Diligence Guidelines; Section 6 of CB Notice No. 3090/2021 (as amended by CB Notice No. 3599/2023), Regarding AML/CFT/CPF Guidelines for Financial Institutions; and CB Notice No. 3156/2022, Regarding, Guidance for Licensed Financial Institutions on the Risks Relating to Payments, outlines the following Customer Due Diligence (CDD) regulatory expectations for SVFs and RPSPs:

1. Identify each customer and verify the customer's identity using documents, data, or any other identification information from a reliable and independent source.
2. Prevent and manage risks related to identity proofing and enrolment, such as the risks of an applicant using falsified identity evidence or another individual's identity.
3. Ensure customer or business relationship risk assessment processes are robust and reliable, and that they incorporate the results of the National Risk Assessment, and their own ML/TF business risk assessment.
4. Undertake ongoing supervision of customers' activity, including monitoring of transactions executed throughout the course of the relationship.
5. Maintain the Customer Due Diligence documents, data and information obtained on customers, and their Beneficial Owners or beneficiaries up to date.
6. Conduct Enhanced Due Diligence measures with regard to customers identified as high-risk, such as politically exposed persons (PEPs) and customers associated with high-risk countries.

Prior to the establishment of a business relationship or the processing of any transaction on behalf of a customer, SVFs and RPSPs are required to fulfil mandatory identification and verification procedures. Additionally, SVFs and RPSPs must understand the intended purpose and nature of a customer's transactions. Throughout the business relationship, these entities are required to monitor transactional activities to ensure it aligns with the customer's established profile and known source of funds.

A review of how SVFs and RPSPs implement Customer Due Diligence (CDD) revealed the following findings:

a) Data analytics of the KYC/CDD submissions showed high levels of accuracy and completeness across most SVFs and RPSPs. However, certain entities failed to correctly capture critical data points, specifically trade license numbers, Emirates ID expiry dates, and passport expiry dates.
b) A Significant portion of the SVFs and RPSPs had adequate processes for the identification of Politically Exposed Persons (PEPs) and performing enhanced due diligence (EDD) process for such customers, as relevant.
c) Analysis of the submitted KYC data confirms that most SVFs and RPSPs perform adequate customer risk assessments. Currently, 57% of all customers have been risk-rated on the basis of the customer risk assessments conducted during onboarding and through periodic reviews. Entities that have failed to meet this standard must now implement these assessments to achieve full compliance.
d) The review noted that most SVFs and RPSPs (71%) had implemented measures to monitor remote access and detect VPN usage. However, a small portion (29%) of the SVFs and RPSPs were developing capabilities to identify VPN usage, and (35%) were working to improve their monitoring of the geographic locations from which services are accessed. Enhancing these technological controls will further strengthen compliance with requirements related to high-risk and sanctioned jurisdictions.



The findings reflect that the majority of SVFs and RPSPs have foundational Customer Due Diligence (CDD) frameworks in place, with identified gaps primarily concentrated in areas relating to digital access controls and enhanced risk differentiation rather than fundamental onboarding failures.

While certain SVFs and RPSPs demonstrated limitations in monitoring access locations and identifying VPN usage, these observations are largely linked to the increasing digitisation of service delivery models rather than a complete absence of customer identification measures. Core KYC processes appear to be operational across the sector, with deficiencies mainly relating to the enhancement and refinement of remote access monitoring capabilities.

Similarly, gaps concerning the variation of due diligence timing for lower-risk customers, application of simplified due diligence, and documentation of CDD review/update processes indicate opportunities to further increase the maturity of risk-based implementation. The relatively lower percentages associated with restrictions on services and expired ID handling suggest that key identification controls are generally embedded, with targeted improvements required to strengthen consistency and documentation.

Overall, the results demonstrate that SVFs and RPSPs are operating with established CDD structures, and supervisory observations are focused on advancing the sophistication of digital onboarding controls, geo-location monitoring, and risk segmentation practices in line with evolving delivery channels. The sector is therefore positioned to enhance the effectiveness of its CDD frameworks through targeted system enhancements and clearer understanding and implementation of risk-based controls, supporting stronger mitigation of ML/TF/PF risks within an increasingly remote service environment.

To mitigate the customer due diligence risks, SVFs and RPSPs should enhance the application of risk-based compliance frameworks that include conducting comprehensive customer risk assessments at onboarding and periodically; ensuring accurate and up-to-date KYC data; and enhancing the application of enhanced due diligence for high-risk relationships. SVFs and RPSPs should strengthen transaction monitoring systems with typology-based detection scenarios, VPN/IP tracking, and jurisdiction monitoring. Ensuring such improvements are made will further enhance controls and reduce exposure to ML/TF/PF risks.

6.2. PAYMENT TOKEN SERVICE PROVIDERS (PTSPs)

6.2.1. Governance and Management Oversight.

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

REGULATORY EXPECTATION.

Article (19) of Federal Decree by Law No. 10 of 2025, Article (21) and (22) of Cabinet Resolution No. (134) of 2025, Article 24 of the Payment Token Services Regulation; and Sections 5, 7 and 8 of CB Notice No. 3090/2021 (as amended by CB Notice No. 3599/2023), Regarding AML/CFT/CPF Guidelines for Financial Institutions, outlines the following governance management oversight expectations:

1. Senior management should set out ML/TF/PF risk appetite and a proper "tone at the top".
2. Senior management of all PTSPs are responsible for performing certain functions related to the assessment, management and mitigation of the ML/TF/PF risks to which their organisations are exposed.
3. Appoint a qualified compliance officer in line with the requirements of the relevant Supervisory Authority;
4. Implement internal policies, controls and procedures that enable them to manage and mitigate the ML/TF/PF risks they have identified in their ML/TF/PF business risk assessment, in keeping with the nature and size of their businesses.
5. PTSPs should put in place comprehensive AML/CFT policies and procedures in accordance with the AML/CFT law and regulations
6. PTSPs should formulate and implement appropriate policies, procedures and controls with regard to staff training.

Effective AML/CFT/CPF implementation under the CBUAE's Payment Token Services Regulation relies on rigorous governance and a robust compliance culture. In accordance with AML/CFT/CPF requirements, PTSPs are required to conduct adequate business risk assessments and establish management structures with clear accountability for identifying, assessing, and mitigating ML/TF/PF risks. To ensure the institution's AML/CFT/CPF framework integrity, senior management must be supported by independent control functions. These functions are responsible for providing objective oversight and ensuring strict adherence to all AML/CFT/CPF obligations.

The review conducted identifies critical areas where PTSPs must prioritize improvements to their governance and oversight frameworks to ensure full regulatory compliance:

a) **ML/TF/PF Business Risk Assessment**: PTSPs are required to conduct comprehensive business risk assessments for ML, TF, and PF within the relevant assessment period. These assessments should aim to identify, evaluate, and mitigate ML/TF/PF risks at the organisational level, covering all products, services, customer segments, and delivery channels.

   During onsite examinations, the CBUAE reviews documentation, examine systems, and interview relevant personnel to verify that risk assessments are performed regularly, are comprehensive and current, and are fully integrated into the PTSP's overall risk management framework.

   As the sector matures, PTSPs are expected to enhance both the conduct and implementation of their ML/TF/PF business risk assessments. Improved risk assessment practices will allow PTSPs to more accurately identify and evaluate both inherent and residual risks across all business areas. This, in turn, will support more informed strategic decision-making and help foster a stronger risk-aware culture throughout the institution, including at both management and Board levels.

   Service Level Agreements (SLAs) with Agents: PTSPs must establish clear, robust SLAs with their Agents, ensuring all AML, CFT, and CPF compliance responsibilities are well-defined, assigned, and actionable. Both PTSPs and Agents must maintain effective controls, transparency, and accountability, with the PTSP retaining ultimate responsibility for compliance. The CBUAE monitors these arrangements to ensure that compliance obligations and escalation mechanisms are explicit, effective, and enforced.

   To address gaps in SLAs between PTSPs and Agents, PTSPs must ensure that, SLAs clearly define the scope of AML, CFT, and CPF requirements, as well as the specific roles, responsibilities, and escalation protocols for both parties. These measures will strengthen governance, enhance clarity of responsibilities, and support a robust compliance culture aligned with regulatory expectations.

6.2.2. Transaction Monitoring Systems.

REGULATORY EXPECTATION.

In line with Article (19) of Federal Decree by Law No. 10 of 2025, Article (17 and 18) of Cabinet Resolution No. (134) of 2025, Article 24 of the Payment Token Services Regulation; and Section 2 of CB Notice No. 4368/2021, Regarding, Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening; PTSPs are required to have an effective transaction monitoring (TM) program that enables the detection, investigation, and reporting of suspicious transactions, in compliance with the UAE's legal and regulatory framework, and ensures that customers and transactions remain within their risk appetite.

A robust and effective transaction monitoring (TM) program is a fundamental component of the AML/CFT/CPF framework for PTSPs, as it enables timely identification and reporting of suspicious transactions to the UAE's Financial Intelligence Unit (FIU). Given the high velocity and pseudonymous characteristics of payment token transactions, PTSPs face elevated exposure to ML/TF/PF risks. A robust and effective transaction monitoring program is therefore essential to detect patterns indicative of illicit activity, including micro-transactions often linked to terrorism financing and rapid layering schemes common in virtual asset misuse.

Given that the sector has only been operational for one year and the AML, CFT, and CPF framework is still developing, only a few areas have been identified for improvement. However, based on early data, PTSPs are expected to focus closely on these specific areas to enhance their compliance efforts:

a) incorporate robust blockchain analytics tools to monitor, trace, and analyse on-chain activities related to any issued payment tokens. These tools should enable PTSPs to effectively identify suspicious transactions, including patterns such as layering, structuring, and obfuscation.

b) fully implement the FATF Recommendation 16 Travel Rule requirements across all aspects of the AML, CFT, and CPF control framework. This will ensure comprehensive compliance with international standards and domestic standards for the accurate collection and secure transmission of originator and beneficiary information for virtual asset transfers.

These measures, supported by clear governance, documented procedures, and phased implementation aligned with the sector's maturity, will significantly enhance the ability to detect suspicious activity and maintain compliance with both international and domestic standards.

7. CONCLUSION

The SVF, RPSP and PTSPs sector has demonstrated a clear and growing understanding of its AML/CFT obligations, with the majority of institutions evidencing structured compliance frameworks aligned to applicable regulatory requirements. Institutions have established documented AML/CFT policies and procedures, conducted Business and Enterprise-Wide Risk Assessments, and embedded governance mechanisms to oversee AML/CFT/CPF risks commensurate with their size and operational complexity. While there are remaining areas for improvements, deficiencies associated with Business Risk Assessments were mostly procedural in nature.

A notable strength across the sector is the formal appointment of Compliance Officers (COs) and Money Laundering Reporting Officers (MLROs) with defined roles, reporting lines, and responsibility for oversight of AML/CFT implementation. In most cases, Cos and MLROs are positioned with appropriate access to Senior Management and Boards, enabling effective escalation of material risks and ensuring accountability within governance structures. This reflects a positive compliance culture and recognition of AML/CFT/CPF as a core regulatory priority.

The sector has also implemented foundational customer due diligence, transaction monitoring, and sanctions screening controls, demonstrating operationalisation of key preventive measures. While opportunities remain to further enhance digital monitoring sophistication and risk-based calibration, the sector overall exhibits a structured approach to compliance, awareness of evolving typologies, and responsiveness to supervisory expectations.

Collectively, these elements indicate that the sector is transitioning from baseline compliance towards more mature, risk-sensitive AML/CFT/CPF frameworks, supported by dedicated compliance resources and increasing alignment with regulatory standards. The sector has shown awareness of their statutory obligations and a willingness to improve. Insights from this thematic review will inform the AML/CFT Supervision Department's ongoing supervisory activities, and will be integrated into future sectoral oversight plans.

8. NEXT STEPS

To strengthen compliance, the sector must address the findings highlighted in this review, and allocate adequate resources to enhance the effectiveness of their AML/CFT/CPF frameworks. Senior management and Boards of Directors are expected to take full accountability for ensuring timely remediation of identified gaps, and embedding a strong compliance culture across their institutions.

Institutions must conduct a comprehensive gap analysis of their AML/CFT/CPF frameworks to ensure full alignment with the requirements of Federal Decree by Law No. 10 of 2025, Cabinet Resolution No. (134) of 2025, and Cabinet Decision No. 74 of 2020, as well as all relevant regulatory notices and guidance. This analysis must be accompanied by a detailed Risk Mitigation Plan and submitted to the CBUAE at amlreporting@cbuae.gov.ae no later than **15 July 2026**. The CBUAE may take enforcement actions against any SVFs, RPSPs, and PTSPs who fails to take adequate steps to address the identified weaknesses and gaps within the stipulated timeframes.

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

ANNEX 1

TYPOLOGIES RELATED TO MONEY LAUNDERING, TERRORIST FINANCING, AND PROLIFERATION FINANCING OBSERVED IN PROVIDERS OF STORED VALUE FACILITIES, RETAIL PAYMENT SERVICES AND CARD SCHEMES

Introduction

The methods used by criminals to launder proceeds of crime, finance terrorism, and support proliferation activities continue to evolve in sophistication, particularly with the increased use of digital payment channels. Stored Value Facility and Retail Payment Service Providers (SVFs and RPSPs), by virtue of their speed, accessibility, and cross-border capabilities, present attractive avenues for misuse.

Accordingly, it is critical that regulated entities operating within this sector maintain robust and dynamic AML/CFT/CPF frameworks, supported by continuous monitoring of emerging typologies. Institutions are expected to incorporate evolving ML/TF/PF risks into their compliance training programmes, customer risk assessments, and transaction monitoring systems.

This Annex outlines key typologies observed within the sector, associated red flags, and recommended mitigation measures.

1. Money Mule

Money mule activity involves individuals who transfer or move illicit funds on behalf of others to obscure the origin of proceeds. Within SVFs and RPSPs, mule accounts are commonly used to rapidly receive, transfer, withdraw, or convert funds into cash or virtual assets.

The report published by the CBUAE on the TYPOLOGIES IN THE FINANCIAL SECTOR under section “Money Mule activity” indicates that the number of “money mules” increased to launder ill-gotten funds, as a result of widespread financial distress.

The CBUAE has identified an increase in money mule activity, driven in part by financial vulnerabilities and the exploitation of individuals.

1.1. Red Flags

- Sudden surge in incoming transfer followed by immediate withdrawals;
- Accounts exhibiting short-term usage followed by dormancy;
- Matching or near-matching incoming and outgoing transaction values;
- IP address or geolocation inconsistent with customer profile; and
- Multiple accounts accessed via the same device or IP

2. Small Cash deposit

Illicit actors may structure transactions into smaller amounts to avoid detection thresholds, particularly when funding wallets or prepaid instruments. These funds are subsequently layered through transfers or converted into other forms.

2.1. Red Flags

- Frequent wallet top-ups within a short period followed by transfers
- Multiple accounts linked to the same address conducting sub-threshold deposits
- Rapid movement of funds to high-risk or cross-border destinations
- Repeated deposits followed by purchases linked to dual-use goods

3. Merchant Front

Merchant fronts are legitimate businesses set up to mask illicit transactions. The merchant processes the payments or accept the deposit on behalf of illicit actors, in the process helping them launder the funds using the SVFs and RPSPs.

3.1. Red Flags

- Newly on-boarded Merchant suddenly starts conducting high volume transactions.
- Unverified physical presence and unclear business activity.
- Multiple merchant accounts tied to one IP or Device
- Transactions not in line with the business activity.

4. Cross-border use for illicit Fund Transfer

SVFs and RPSPs facilitate efficient cross-border payments, which may be exploited for illicit fund transfers, including sanctions evasion and layering activities.

4.1. Red Flags

- Transactions involving high-risk or sanctioned jurisdictions
- Transaction volumes inconsistent with customer profile
- Use of VPNs or high-risk IPs to initiate transactions
- High-velocity cross-border merchant category (MCC) activity
- Geofencing breaches or attempts to bypass restrictions

5. IP Manipulation / Geo Spoofing

Users may employ VPNs, TOR networks[4], or other anonymisation tools to mask their true location, potentially indicating attempts to circumvent sanctions or obscure illicit activity.

5.1. Red Flags

- Use of VPN or TOR networks, or anonymizer to mask IP or location
- Frequent IP address change in short period of time.
- Same IP address or device to access multiple unrelated accounts.
- Time Zone mismatch between transaction timestamp and device or IP time zone.
- Access attempts from known blacklist IPs.

6. Recommended Mitigation Measures

SVFs and RPSPs are expected to implement proportionate and risk-based controls such as:

- Conducting Enhanced Due Diligence (EDD) on high-risk customers, merchants, and wallets
- Implementing IP tracking and geofencing controls, particularly for sanctioned and high-risk jurisdictions
- Monitoring IP usage in jurisdictions bordering sanctioned countries
- Screening customer devices, counterparties, and transactions against sanctions and proliferation lists
- Developing robust customer and merchant risk scoring models
- Monitoring transactions linked to dual-use goods and high-risk trade activities
- Enhancing oversight of sectors such as freight, logistics, and cross-border trade
- Implementing real-time transaction monitoring and risk scoring, incorporating factors such as geography, customer profile, transaction value, and purpose

[4] The Tor network is designed to protect users' privacy and anonymity on the internet by concealing their location and online activity.

CONCLUSION

While SVFs and RPSPs play a critical role in financial inclusion and digital innovation, they remain exposed to evolving ML/TF/PF risks. The typologies identified highlight the need for continuous enhancement of monitoring capabilities, data analytics, and risk-based controls.

Institutions are expected to proactively identify emerging threats, strengthen internal controls, and ensure ongoing staff awareness to effectively mitigate financial crime risks within the sector.