Annex

Observations and Regulatory Expectations of Stored Value Facility Licensees' Anti-Money Laundering and Counter-Financing of Terrorism Controls over Prepaid Card Business

Background

While the nature and scope of money laundering and terrorist financing (ML/TF) risks in the stored value facility (SVF) sector differs from that in the banking sector, the requirement for SVF licensees to adopt a risk-based approach in the design and implementation of anti-money laundering and counter-financing of terrorism (AML/CFT) systems is the same. It means that each SVF licensee's system should be commensurate with its ML/TF risks, taking into account the nature, size and complexity of the business.

The majority of the SVF sector is characterised by lower ML/TF risks in view of low stored values, limited functionality and predominant use for transport and low-value retail transactions[1] and where this is the case, a basic system may suffice. However, as business models evolve, higher ML/TF risk situations sometimes emerge, such as prepaid cards being misused for cash withdrawal in higher risk jurisdictions[2]. In such cases, it is important that these ML/TF risks are identified and assessed, and that SVF licensees understand how their AML/CFT systems are effective in managing these risks. Where gaps are identified, suitable changes should be made to the system.

The Hong Kong Monetary Authority (HKMA) has recently completed thematic reviews of the AML/CFT systems of a number of SVF licensees whose SVF business primarily involved the issue of prepaid cards. This note provides feedback from these reviews, including key observations as set out below and general regulatory expectations provided in text boxes.

---

1 As indicated in the "Stored Value Facility Sector: Money Laundering and Terrorist Financing Risk Assessment Report" published by the HKMA on 19 July 2019 (https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190719e1.pdf).

2 An SVF licensee should assess the risk of jurisdictions it is exposed to, especially in relation to jurisdictions identified by credible sources as having relatively higher levels of corruption or organised crime, and/or not having effective AML/CFT regimes. Reference should also be drawn to statements on "High-Risk Jurisdictions subject to a Call for Action" and "Jurisdictions under Increased Monitoring" issued by the Financial Action Task Force (FATF).

Annex

1. AML/CFT control system and ML/TF risk assessment

Institutional ML/TF risk assessment

1.1. All SVF licensees reviewed have conducted institutional ML/TF risk assessments to identify, assess and understand the ML/TF risks of their businesses, based on customer, product, geographical and channel risks, and have established basic AML/CFT control systems which are largely commensurate with those risks. As a developing sector, the approach to risk assessment varies. Some institutional ML/TF risk assessments included quantitative analysis (e.g. number of high-risk customers, breakdown of customer base and transactions by jurisdictions, customer usage behavior) to support the risk analysis, and were able to illustrate the appropriateness and effectiveness of relevant risk mitigating measures.

1.2. Where risk assessments contained less quantitative and qualitative analysis to support the assessment of the risk factors, the evaluation of the appropriateness and effectiveness of AML/CFT controls was adversely impacted. We noted some risk assessments were largely static and had not evolved in response to threats which had arisen either from the original or changed business models.

1.3. Some assessments of AML/CFT control effectiveness were found to be mostly descriptive and focused on whether the control framework was in place; greater consideration of the adequacy and effectiveness of the controls in mitigating the ML/TF risks identified would add value to the usefulness for SVF licensees.

Product ML/TF risk assessment

1.4. In general, SVF licensees conducted the relevant risk assessments before launching new products and services or introducing new business practices and took appropriate measures such as imposing transaction limits (e.g. cash top-up and withdrawal limits) to manage and mitigate identified risks.

1.5. In a few cases, room for improvement was noted in how SVF licensees

assessed the inherent ML/TF risk factors related to new products prior to launch, as well as services and customers where changes had been made to the business model. For example, an SVF licensee introduced a major change to its customer on-boarding arrangement without adequately assessing how the new arrangement contributed to an increased ML/TF risk profile, and as a result did not take adequate measures to mitigate relevant risks (e.g. impersonation risk).

Regulatory Expectation

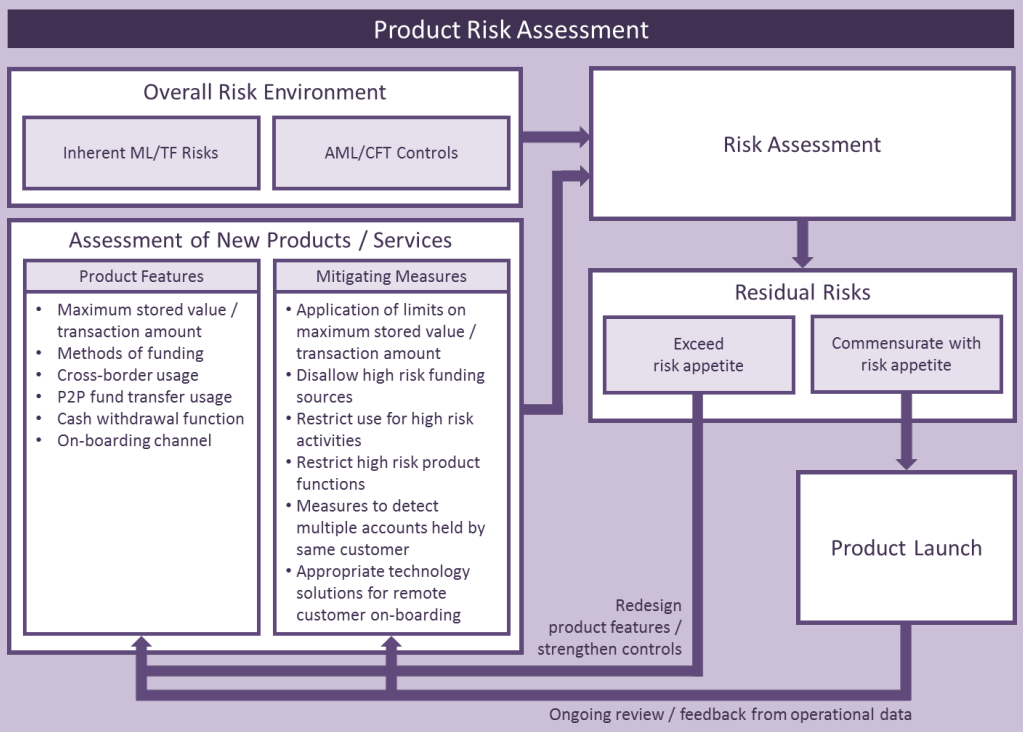
- Implementing an effective AML/CFT control system requires adequate understanding of ML/TF threats, vulnerabilities and risks[3]. The ML/TF risk assessment forms the basis of the risk-based approach, enabling an SVF licensee, whatever the nature, size and complexity of its business, to understand how and to what extent it is vulnerable to ML/TF, and what commensurate measures it should take.
- The level of detail contained in the institutional ML/TF risk assessment, including the process of identifying and assessing relevant risks and qualitative/quantitative analysis, will vary depending on the nature and business size of individual SVF licensee, and at a minimum, should take into account relevant information regarding key risk factors.
- SVF licensees should stay vigilant to emerging ML/TF risks (such as the increasing sophistication of criminal networks that seek to circumvent licensees' controls) which may arise in their business or the sector as a whole and should regularly update the risk assessment.
- When feedback and guidance are provided by the HKMA or the Joint Financial Intelligence Unit (JFIU), or where typologies information is received from the Fraud and Money Laundering Intelligence Taskforce (FMLIT)[4], SVF licensees should assess whether the risk and/or vulnerability is already addressed in existing control systems and if not, what enhancement is required.
- It is a specific regulatory requirement that SVF licensees should

[3] SVF licensees may make reference to the "FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment" issued in February 2013, where the principles described in the guidance are also relevant to more focused risk assessments. In addition, reference could also be drawn to the "Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services" issued by the FATF in June 2013.

[4] FMLIT was established in 2017, led by the Hong Kong Police Force with participation by the Hong Kong Monetary Authority and a number of retail banks. Similar to arrangements in other international financial centres, FMLIT targets current and emerging financial crime threats by adopting a public private partnership approach to information sharing, both at the strategic and tactical level.

undertake adequate risk assessments before launching new products or business practices, or introducing new or developing technologies.

- SVF licensees should develop assessment framework for the capabilities of AML/CFT systems and controls (such as transaction limits, taking into account customers' previous usage data and patterns) and use that understanding and assessment results to regularly enhance effectiveness in execution.
- A general approach of product risk assessment is provided in the chart below:



2. Managing AML/CFT controls in relation to engagement with co-brand partners and distributors

2.1. It is common practice for SVF licensees issuing prepaid cards to engage business partners (e.g. co-brand partners and distributors[5]) in selling their prepaid cards. Under such arrangements, the business partners may assist the SVF licensees in collecting customer information such as

[5] Co-branding is a partnership between the SVF licensee and the co-brand partner in the form of co-brand prepaid card, leveraging the customer base of the co-brand partner. The co-brand prepaid card is customized with company brand of co-brand partner and presented with a printed logo of both the co-brand partner and the card issuer (i.e. SVF licensee). Besides, distributors assist the sales distribution of prepaid cards (e.g. gift cards) on specific sales outlets such as convenience stores.

identification documents, distributing prepaid cards to customers and handling certain top-up transactions under a contractual relationship between the SVF licensee and business partner. However, since SVF licensees do not deal with the customers directly, they have to rely upon the business partners to perform certain controls (such as identity authentication and verification, identification of source of top-up funds) on their behalf. In such cases, the SVF licensee should apply effective controls to ensure business partners act according to the licensee's procedures in practice to address the increased vulnerabilities of such arrangements.

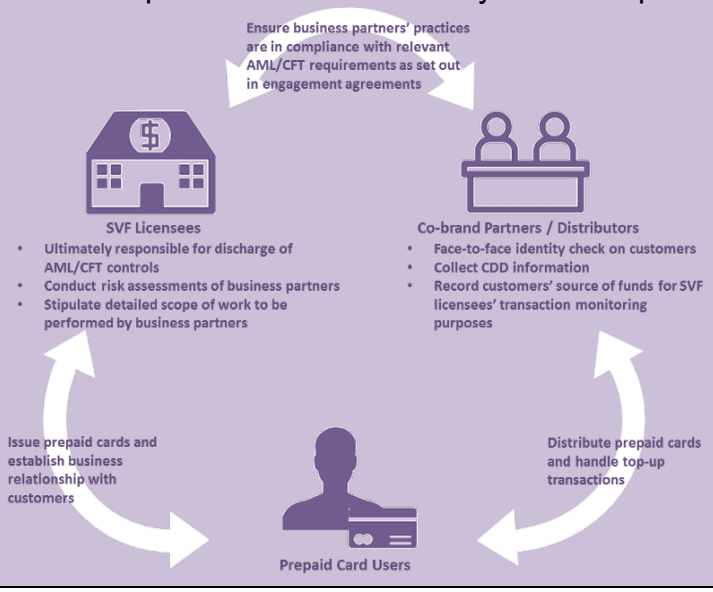
2.2. The use of co-brand partners and distributors chain can make implementing adequate AML/CFT controls and oversight more challenging. While it is well understood that the ultimate responsibility for ensuring that AML/CFT controls are adequately applied rests with SVF licensees, the thematic review noted that in some cases oversight of business partners' systems and ongoing performance, to ensure the legal and regulatory obligations were met and ML/TF risks were adequately managed, had not always been effectively implemented. Key observations are summarized below.

- Some SVF licensees did not always conduct adequate risk assessments before engaging a business partner to understand the latter's business nature and the risk of a particular type/group of customers to be referred by the business partner, and how this contributed to changes in the risk profile of SVF licensee concerned;
- Not all business agreements between SVF licensees and their business partners clearly stipulated the required scope of work (e.g. types of customer due diligence (CDD) information required, identity check on customers, acceptable top-up channel, record-keeping of source of top-up funds) to be performed by the business partners on behalf of the SVF licensees;
- In some cases, SVF licensees did not require their business partners assisting in handling top-up transactions to obtain the source of top-up funds where appropriate or to pass such information to the SVF licensees for transaction monitoring purposes; and
- In some cases, SVF licensees had not conducted reviews to ensure that their business partners' practices were in line with the SVF

licensees' procedures and in compliance with the relevant AML/CFT requirements.

Regulatory Expectation[6]

- As the issuer of SVF products who maintains the business relationship with a customer, the SVF licensee bears the ultimate responsibility for ensuring that relevant AML/CFT controls are adequately applied regardless of whether its business model involves operating through business partners.
- SVF licensees should implement appropriate arrangements to ensure that operations conducted through business partners do not compromise the effectiveness of their AML/CFT controls. Such arrangements should include, but are not limited to:
  - conducting adequate risk assessments before engaging a business partner, including understanding the latter's business nature and the risk profile of customers who may be referred by the business partner;
  - ensuring that the respective roles and responsibilities are clearly set out in the contractual agreements with business partners; and
  - seeking adequate assurance of the effective implementation of the SVF licensees' procedures by the business partners and regularly verify that these are effectively applied in practice in line with the agreement, such as through regular performance reviews and quality checks on CDD processes carried out by business partners.



6 These principles are also applicable to SVF licensees where similar arrangements are being used relating to AML/CFT controls, such as outsourcing or agency relationships.

3. Customer risk assessment (CRA) and customer due diligence

3.1. The adequacy of customer identification policies, and record keeping were stronger aspects of the review; basic CDD frameworks had been established in accordance with the requirements in the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Stored Value Facility Licensees). Furthermore, all SVF licensees reviewed had established CRA frameworks to assess and assign ML/TF risk rating for a business relationship.

3.2. The review noted that implementation of some aspects of effective CRA and CDD control measures are challenging for some SVF licensees, particularly where higher risks were encountered. The control issues identified were mainly attributable to the limited overall ML/TF risk awareness of senior management and compliance functions[7], insufficient understanding of how control systems (including the CRA system and the transaction monitoring (TM) system) could mitigate these risks, especially for high risk situations, or a lack of adequate policies and procedures. For example, failing to regularly update internal reference data on high-risk jurisdictions for risk assessment processes can undermine the effectiveness of relevant AML/CFT controls.

3.3. The review examined a case in which a customer made relatively substantial payments for goods and services in various jurisdictions. While the system worked correctly to flag these significant transactions, the SVF licensee might not have taken appropriate actions, e.g. obtaining further information on the customer's background such as occupation and business nature, and source of funds, to assess the customer risk profile and transactions. This was attributable to a number of factors, including insufficient risk awareness and shortcomings in policy and procedures.

Regulatory Expectation
• Apart from maintaining sufficient risk awareness and adequate understanding of control systems performance, SVF licensees should establish adequate internal procedures and provide sufficient guidance and training to staff to enable them to undertake CRA and CDD

[7] Some small SVF licensees have less relevant experience to implement an effective risk-based approach.

measures effectively.

- The compliance function should conduct regular reviews to monitor the effectiveness of relevant controls and, where necessary, make suggestions to senior management to enhance controls and procedures.
- While the CRA assists the SVF licensee to apply appropriate and proportionate CDD and risk-mitigating measures, the SVF licensee should also recognize that, for some customers, risks may only become evident through ongoing monitoring after the customer has commenced using the SVF product. SVF licensees should therefore update risk assessments of customers from time to time based on any additional information.

4. Transaction monitoring

4.1. All SVF licensees reviewed had implemented TM systems[8] to monitor customer activities, taking into account the nature, size and complexity of their businesses. The review noted that TM systems could in general flag comparatively simple scenarios and transactions for further examination, although their capacity to monitor and capture more complex scenarios could be improved.

4.2. The TM systems adopted by SVF licensees were either self-developed in-house or developed by external vendors. The review observed that in some cases licensees' understanding of the TM systems was not sufficient, which may be attributable to licensees' over-reliance on the external service providers in developing and managing the systems without adequate knowledge transfer to relevant staff, or changes of compliance staff responsible for in-house TM systems without sufficient documentation of system information to ensure continuity. In one case, certain functions of the TM system had not been activated by the licensee due to lack of understanding of the system and, as a result, certain types of transactions were not captured by the system, creating an effectiveness gap of which the SVF licensee was not aware of.

4.3. It is widely accepted that ML/TF risks can increase when the ability to

[8] Including management information system (MIS) reports.

withdraw cash is offered, and this function should be subject to monitoring. Where this service is offered overseas, the ML/TF risks will generally be higher. Our review noted that monitoring of the pattern of cash withdrawal transactions overseas was generally inadequate, e.g. large amounts of cash withdrawn shortly after top-up and frequent and substantial cash withdrawals. These transactions were generally monitored based on reports of single large transactions or by geographical locations. Such an approach appeared ineffective in flagging potentially higher-risk patterns of transaction for further review to understand their background and purpose.

4.4. The review also noted that, while SVF licensees conducted regular reviews of TM systems, the scope of reviews was often limited and unable to adequately assess the effectiveness of TM systems in identifying unusual transactions.

4.5. The quality and consistency of TM alerts and reports clearance and investigation varied among SVF licensees. A common issue identified was that the justifications for TM alerts and reports clearance were not always documented or were insufficient. In one case, while the system correctly flagged unusual transaction patterns of frequent and substantial cash withdrawals in a particular overseas country, the potentially higher risk of these transactions was not understood and insufficient action was taken to analyse the relevant customer profiles and purpose of transactions to assess whether the transaction pattern matched the SVF licensee's knowledge of the relationships involved. The SVF licensee simply accepted customers' explanation (e.g. cash withdrawal for overseas travel) despite an emerging pattern of frequent and substantial cash withdrawals conducted by a number of customers in the particular overseas country and which appeared to have no logical economic purpose.

Regulatory Expectation
• SVF licensees should ensure that relevant staff have sufficient understanding of TM system performance, whether they are developed in-house or provided by external vendors. Licensees should provide appropriate and regular training to staff to ensure that they have appropriate skills and knowledge to implement and operate TM systems

effectively.

- SVF licensees should regularly review the adequacy and effectiveness of their TM systems and processes, taking into account their risk assessments, and ensure that the systems are appropriate to their operations and context. The review should include handling of TM alerts, coverage of scenarios (e.g. pattern of frequent and substantial cash withdrawal in foreign jurisdictions), and parameters and thresholds adopted, taking into account previous business operating data. Where an SVF licensee plans to launch new products and functions, consideration should be given to developing additional TM scenarios and MIS reports.
- SVF licensees should refer to the "Guidance Paper on Transaction Screening, Transaction Monitoring and Suspicious Transaction Reporting" issued by the HKMA as an important reference for the review process. Although developed with inputs from banks, the guidance paper is equally applicable to the SVF sector. It provides a relatively high-level summary of all major principles and considerations which the HKMA will focus on and examine regarding the design and implementation of a TM system.
- As criminal techniques and ML/TF risks evolve over time, SVF licensees should make reference to the latest typologies available[9] and conduct regular reviews to ensure their TM systems continue to be effective.
- Prior to major changes to TM systems, such as introducing additional MIS reports or TM scenarios, SVF licensees should conduct adequate testing and validation to ensure the TM system is operating as intended or designed.
- In respect of TM alerts and reports clearance processes, the SVF licensee should consider whether it is satisfied with customers' explanation of the transactions and should not accept at face value insufficient and simplistic explanation, which are unable to resolve the grounds for suspicion. SVF licensees should also achieve a correct balance between detail and efficiency.

[9] E.g. typologies and alerts shared by the HKMA, the JFIU and the FMLIT.

5. Name screening

5.1. SVF licensees had implemented name-screening systems which made use of commercial databases to conduct on-boarding and regular customer name screening to identify potential designated parties and politically exposed persons. These were generally well implemented although in one case, the effectiveness of the name-screening system might have been undermined by inappropriate settings. This was due to the concerned SVF licensee largely relying on the solution provided by the external vendor without developing sufficient knowledge and understanding of the operation of the name-screening system.

5.2. Similar to the issues identified in handling of TM alerts, justifications for name-screening alert clearance were not always documented and sometimes insufficient.

Regulatory Expectation
• SVF licensees should recognise that the responsibility to implement effective name-screening systems lies with the SVF licensees, not with its vendor. • SVF licensees should provide appropriate and regular training to staff to ensure that they have appropriate skills and knowledge to implement name-screening systems effectively. Also, SVF licensees should conduct regular testing and validation to ensure that the name-screening system is operating as intended or designed. • SVF licensees should refer to the "Guidance Paper on Transaction Screening, Transaction Monitoring and Suspicious Transaction Reporting" issued by the HKMA as an important reference when conducting regular reviews of name-screening systems.