the
Wolfsberg
Group

Wolfsberg Group Guidance on the Provision of Banking Services to Fiat-backed Stablecoin Issuers

Introduction

The increased adoption of fiat-backed stablecoins represents a new financial crime risk management challenge to financial institutions (FIs). Stablecoin features offer significant legitimate benefits for individuals and businesses worldwide, however these same attributes of price stability, global reach, pseudonymity, and rapid settlement also make them attractive to illicit actors, allowing them to access major currency denominated value without engaging traditional payment rails, including in sanctioned jurisdictions. At the same time, the increased ability to trace and, in some cases, freeze transactions presents a compliance challenge to FIs on where to draw the line with respect to oversight and monitoring. The Wolfsberg Group believes that most of the same financial crime risk management principles apply in developing and monitoring a relationship with any type of bank or non-bank financial institution, which is reinforced in this document. However, this guidance also explores the unique financial crime risks associated with the provision of banking services to a fiat-backed stablecoin issuer operating in a regulated jurisdiction and establishes a framework for FIs to manage these relationships appropriately.

The guidance begins by introducing the relevant terminology used by the Group on stablecoins. While definitions may differ across the industry, a shared understanding of the basic terms introduced and explained here will be relevant for developing the overarching risk management framework. The guidance then describes the typical fiat-based services that an FI may provide to a stablecoin issuer, emphasising how existing financial crime-related controls may require tailoring to respond to the unique risks presented by the relationship. The guidance then goes on to describe the level to which an FI, in following a risk-based approach, may monitor the compliance obligations of the issuer on the blockchain.[1]

Ultimately, the conceptual approach to banking a stablecoin issuer is similar to any customer relationship. An FI should understand the risks associated with the customer and the relationship, as well as how that customer manages those risks. The FI then should determine if

[1] The Group uses the term blockchain here and throughout the guidance for consistency. The guidance should also apply to stablecoins developed using other forms of distributed ledger technology (DLT).

it is comfortable both with the risk exposure and risk management strategy offered by the issuer. Finally, the FI should develop a reasonable risk management framework that allows the FI to determine if the customer's behaviour stays within that appetite and take corrective action as necessary.

A common understanding of fiat-backed stablecoins

As shared in the Wolfsberg Group's FAQs on Defining Digital Assets, the Group considers stablecoins to be "a digital asset, token or form of digital cash that is designed to maintain a stable value or peg its market value to some external reference relative to a specified asset or a pool or basket of assets including fiat currency". In this guidance, we only consider stablecoins that are issued by a corporate issuer, pegged to a fiat currency and fully backed by reserves, which are liquid assets, denominated in the same currency as the stablecoin (for example, cash, demand deposits, short-term government bonds or high-quality commercial paper). These present minimum market and credit risk and are approved by prudential authorities (referred herein as "fiat-backed stablecoins"[2]). Fiat-backed stablecoins should be distinguished from "other stablecoins", such as those referencing other types of assets (e.g., gold or silver) or algorithmic stablecoins[3], and classified separately from a money laundering/terrorist financing (ML/TF) risk perspective. We do note, however, and discuss further below, that reserve-backed assets can and do pose their own ML/TF risks.

A **stablecoin issuer** is an entity that issues and redeems stablecoins and is responsible for ensuring they are backed by reserve assets to enable ongoing redemption at par value. The issuance and redemption cycle of a fiat-backed stablecoin should ensure that each token remains fully backed by the reserves described above.

When a client purchases a stablecoin from the issuer, typically by paying with bank deposits, an equivalent amount of stablecoins is issued or "minted", and the purchase is settled by the issuer transferring the stablecoin to the client's wallet (**minting**). "Client" here refers to the client of the issuer who then distributes the stablecoin (typically a digital asset service provider or DASP, discussed in detail below), not the many "users" of the stablecoin (who could be natural persons, businesses, etc). For example, a 1 USD deposit payment results in the minting of one new USD-backed stablecoin, increasing the amount in circulation. The issuer uses the proceeds from the stablecoin purchase to hold reserve assets to maintain a 1:1 peg. When a client wishes to redeem stablecoins, they transfer the tokens back to the issuer's wallet. In those cases where a direct client of an issuer conducts a redemption, these tokens are then destroyed (**burning**) and the corresponding amount, typically in bank deposits, is transferred from the reserve and returned to the client. This reduces the circulation supply, maintaining the balance between tokens and reserves.

There are situations, however, where the issuer may opt to purchase the stablecoins without burning them, using, for example, their own cash reserves. In this case, the redemption does not result in a reduction of the stablecoin supply in circulation. Additionally, in certain situations – such as the fulfilment of court orders, regulatory actions, or restitution to fraud victims – issuers may burn stablecoins and subsequently reissue them to authorised parties. This reissuance

[2] Synonymous terms here would include "fiat-pegged stablecoins", "payment stablecoins", and "electronic money tokens", as long as the stablecoin is denominated in a fiat currency, is not a digital asset that is itself a national currency, and the issuer holds high quality liquid assets to back its obligation to redeem the stablecoins into fiat or bank deposits.
[3] Algorithmic stablecoins, as an example, do not hold reserves and utilize a set of pre-programmed rules and smart contracts to maintain circulating supply and its peg. See the *Wolfsberg Group Frequently Asked Questions (FAQs) on Defining Digital Assets* (2024) for more details on other stablecoin types.

ensures that assets frozen or destroyed as part of an enforcement action can be restored or transferred in accordance with the relevant legal requirements.

Understanding and monitoring the purpose and intended nature of the business relationship

The standard services provided by an FI to an issuer are operating accounts, reserve accounts and settlement accounts for transactions related to the issuer's clients. As in any relationship where an FI provides services to another FI (here, the issuer), a general understanding of the issuer's financial crime risk management framework is foundational to establishing the relationship. Although there are relevant differences between a traditional correspondent relationship and a relationship with a stablecoin issuer, the Wolfsberg Group has issued the Financial Crime Compliance Questionnaire (FCCQ) and the more extensive Correspondent Banking Due Diligence Questionnaire (CBDDQ) to support the assessment of any type of financial institution's financial crime risk management framework. Additional questions and themes unique to a stablecoin issuer are included and explained within this guidance, to complement the financial crime risk management framework categories captured in the FCCQ and CBDDQ.

Beyond the overall financial crime risk management framework, the FI should understand, in advance, the intended purpose of each account and associated product, the expected fund flows to and from the account, and the types of counterparties with which the issuer will interact (the issuer's "clients"). FIs should distinguish here between the issuer's direct clients – such as DASPs, corporates, or non-bank payment service providers (PSPs) – and the "users" who may ultimately receive stablecoins through those intermediaries. Establishing a clear understanding of the stablecoin business model in advance will permit the FI to identify unusual or unexpected activity better, which may represent an evolution of the business relationship, the misuse of certain product types (e.g., in failing to appropriately segregate activities by account type), or in the extreme, indications of suspicious activity, including fraud.

The overall financial crime risk management framework

Baseline principles apply in understanding the maturity of the stablecoin issuer's financial crime risk management programme, with some nuances specific to the issuer's unique risks which may be evaluated together in totality:

- The jurisdictions where the issuer is established and the strength of the regulatory regimes in those countries (including prudential standards), and how the issuer addresses the risks faced by nascent or undeveloped regulatory frameworks for digital assets in otherwise low-risk jurisdictions;
- Consider whether the licensing and supervision is appropriate for the type of activity the stablecoin issuer undertakes and what level of comfort supervision may provide on the regulatory accountability of the stablecoin issuer;
- The establishment of AML/CFT, sanctions, and anti-corruption and bribery (AB&C) frameworks, developed through policies and procedures and executed through dedicated headcount/appropriate resourcing and experienced/competent staff, and the relationship between the financial crime risk management programme and the issuer's programme against fraud;
- Engagement with the issuer's Board or senior management on financial crime related themes, including the approval of the issuer's policies and procedures, and the articulation of the issuer's financial crime risk appetite, for example (non-exhaustive) prohibited/restricted activities, client types and geographic locations, and the methodology used to risk rate clients;

- The degree to which the issuer relies on third parties to satisfy certain elements of the overall financial crime risk management programme, along with the adequacy and soundness of the issuer's framework for evaluating the suitability and effectiveness of those third-party arrangements;
- Established procedures for prompt, cooperative engagement with law enforcement agencies, including designated points of contact, and capabilities to respond to legal orders such as freezes, burns, and reissuance;
- The degree to which the issuer conducts due diligence on its partners and distributors (as part of, for example, the issuer's approach to periodic review). In cases where clients act as distribution channels, the FI should consider whether the issuer has appropriate controls to manage financial crime risks at both layers, including due diligence on intermediaries and visibility into downstream usage patterns;
- The degree to which the issuer conducts due diligence on the blockchains where it decides to issue stablecoins, on areas such as transparency, level of centralisation, permissioned/permissionless blockchains, and any other features which may make the blockchain more susceptible to illicit activity;
- The application of a risk-based approach by the issuer, stemming from an enterprise-wide risk assessment, including risk-based due diligence and enhanced due diligence;
- The monitoring and reporting programme designed to ensure suspicious activity is identified and filed with the relevant competent authorities, including the use of robust in-house or vendor blockchain analytics solutions and the issuer's approach for monitoring activity on blockchains not covered by vendors. This includes the degree to which the risk rules applied within these solutions are customised to align with the issuer's specific business model and the unique risks they face;
- The screening of activity to ensure compliance with sanctions, the sanctions programmes recognised by the issuer, and the issuer's ability to freeze stablecoins associated with sanctioned wallets, sanctioned entities or persons, or subject to subpoena (often referred to as "freeze and seize"), and under what conditions;
- The issuer's commitment to payment transparency standards;
- The compliance testing and oversight approach, including the role of internal audit and assurance teams;
- The issuer's strategy on training and education, to ensure staff across the institution recognise and assume their own roles and responsibilities in managing financial crime risk; and
- How the issuer's financial crime risk management programme integrates with the FI's own risk management and oversight approach, including, for example, the process for ensuring the issuer responds adequately to requests for information (RFIs) initiated by the FI.

It will be important for FIs to monitor changes in the regulatory landscape for stablecoins relevant to the issuers they support, and equally to monitor, as part of the risk management approach, how the issuers themselves maintain compliance with evolving licensing, AML/CFT standards, and disclosure requirements across the jurisdictions in which they operate.

Operating accounts

Operating accounts are used for the issuer's business expenses and operational transactions, such as payroll, vendor payments and services. The account holds the issuer's own funds, not client funds, and is separate from client or reserve accounts. Operating accounts facilitate standard commercial banking activities unrelated to token issuance or redemption, and traditional monitoring approaches apply (especially to ensure operating activity remains segregated from reserve management or client settlement). The risk here is similar to that of an FI providing operating accounts to a non-bank financial institution (NBFI) where the relationship begins as operational but, over time, the NBFI begins to use the accounts to manage third party payments without notification.

Reserve management

Reserve accounts hold the permissible reserve assets backing the issuer's obligation to redeem its stablecoins at par. They hold backing funds and support liquidity or asset acquisition but are not used for direct settlement. When the clients of the issuer (not the end users) purchase newly minted stablecoins, those permissible assets – at least equivalent to the par value of the purchased stablecoins – are placed into the reserve account. These assets are meant to remain segregated from the issuer's other assets and may be subject to regulatory oversight, attestation and audit. Stablecoins are typically burned when redemptions occur, and the corresponding amount is paid from the reserves by the issuer to the redeeming client, indirectly through a settlement account. Generally, the FI would expect the transactional activity behind the reserve accounts to be limited to incoming/outgoing transactions from the settlement accounts, as well as any transactions related to reserve management, for example intra-group activity among different reserve accounts or activities related to permissible reserve assets such as government bonds. Depending on the regulatory framework where the issuer operates, a portion of the funds from the issuer's reserves can be allocated to these liquid financial instruments, including a fund set up by the issuer that is then managed by a third-party asset management firm. Fiat custodians in this sense would be responsible for safekeeping the assets but would not manage them, while asset managers may be appointed to make investment decisions within defined risk and compliance parameters.

The FI should understand the expected reserve management activity, including the issuer's approach to reserve management and whether internal and external audits have been mandated, in order to tailor a monitoring approach aimed at identifying unusual or unexpected activity. On-going monitoring to confirm the proper segregation of accounts, as well as gain comfort that the issuer's claims on reserves are accurate, are critical.

Client settlement

Settlement accounts are controlled by the issuer and facilitate the receipt and disbursement of client funds or reserve assets during the minting and redemption process. When the client initiates a deposit payment to purchase stablecoins, the funds are deposited in the settlement account, which is an account in the name of the issuer established for this purpose. After verification, and once the stablecoins are minted, the funds would be moved to the reserve account for investment and longer-term management. During redemption, the funds are transferred from the reserve account to this settlement account before being sent to the client. The settlement account ensures the operational separation of funds and supports accurate reconciliation and reserve management. Unlike a reserve account, where transactional activity is mainly among accounts all in the issuer's name, or an operating account, where the issuer's counterparties are limited, settlement accounts are exposed to various external counterparties. It is these accounts that present the greatest financial crime risk to an FI, as the fund flows to/from different clients of the issuer will demonstrate the degree to which the issuer is operating within the financial crime risk appetite shared and agreed with the FI.

Similar to managing relationships with PSPs, the FI's approach at onboarding is to understand the issuer's own risk appetite and how the issuer manages that appetite. The FI will want to understand who the issuer's clients are, whether they are DASPs of a certain size, or a combination of DASPs and institutional clients, such as NBFIs, banks, or large corporations or non-profit organisations that intend to employ stablecoins for their own purposes, such as treasury management. The FI will also be interested in the underlying source of funds, how the issuer assesses the compliance framework of these clients as part of their own onboarding and on-going monitoring process, as well as the issuer's appetite on the jurisdictions and associated regulatory regimes where the issuer's clients operate. How the issuer oversees the commitments made by its clients and what payment flows are expected to/from the different account types – recognising that these can be complex – will also be key information to obtain.

The FI's objective is to determine if the issuer's appetite for risk and subsequent management of that risk are sufficiently aligned with the risk that the FI is willing to undertake in providing the issuer with banking services. There may be certain products that the FI prefers not to offer at first, or there may be certain segments of the issuer's client base that the FI does not want to serve (akin to an opt-in/opt-out approach for PSP relationships where an FI's own risk appetite may require a carveout to ensure transactions from certain client types are not routed through the FI). Additional, less-traditional aspects of the issuer's compliance framework to explore would be, for example:

- The minting/burning approach for client settlement and how this will manifest itself in the transactional activity of the settlement accounts. Questions on whether the approach is the same for all client types and whether redemption between the issuer and the client will always occur through a DASP (likely leading to "bulk" redemption from a DASP), or whether some client types (e.g., large corporates) could engage in redemption directly with the issuer, will need to be asked. It is to be noted that, depending on the jurisdiction, the regulatory framework may require the issuer to engage in direct redemption on demand;
- The approach employed by the issuer to determine those DASPs and/or institutional clients with whom the issuer forms a relationship, including, for example, whether compliance with standard payment transparency regulation (often referred to as "the travel rule") is required or expected, and if so, whether the issuer has implemented the necessary processes and tools to comply;
- The degree to which the issuer conducts on-chain monitoring of stablecoin circulation that extends beyond direct business relationships, whether the approach is built in-house or through a vendor, and how the approach changes based upon the type of blockchain to be used and/or when the DASP is considered more/less risky;
- Implementation by the issuer of enhanced monitoring, screening, and controls for stablecoin transfers to or from unhosted wallets that transact directly with the issuer (if applicable);
- Other proactive measures adopted by the issuer to manage financial crime risks, which may include the implementation of on-chain, real-time, pre-transaction verification of wallet addresses and transaction blocking through smart contracts and technological tools. These measures may include pre-transaction deny-list screening, allow-listing of approved addresses, reversible transactions (e.g., delayed settlement with cancellation windows), or other techniques designed to prevent or reverse transfers to high-risk or illicit wallets; and
- The appetite for the issuer to mint/burn stablecoins to/from DASPs with certain levels of activity tagged to predicate offenses or the use of privacy-enhancing tools.

Here, and similar to providing services to other PSPs, the account activity review (AAR) is a standard approach for assessing whether the issuer's fiat-based activities are consistent with the relationship as agreed at onboarding. The frequency of the review may be adjusted for the risk the relationship represents (quarterly, annually, etc.). More advanced FIs may be able to automate aspects of the AAR into a dashboard or similar, while FIs without such capabilities may implement structured manual reviews, ensuring they occur at a frequency appropriate to the issuer's risk profile, with proper documentation and escalation procedures. Identified deviations from the agreed-upon purpose and nature of the relationship (for example the provision of minting/redemption services to a DASP headquartered in a high risk third country, when it was agreed that such activity would not be channelled through the FI) should prompt questions with the issuer, leading to corrective action or possibly the termination of the relationship.

Monitoring the on-chain activity of the issuer's stablecoin

Perhaps the most unique challenge facing an FI in providing services to a stablecoin issuer is the degree to which the FI should engage in the on-chain monitoring of activity. Given the public nature of many blockchains, on-chain monitoring could be a limitless endeavour, and such monitoring, without relevant insights, could be misleading. Instead of assessing the risk and framing the associated oversight according to degrees of transactions on the blockchain since issuance (e.g., "one hop, two hops"), the approach to compliance monitoring should be focused on the single question of whether the issuer is operating within its own risk appetite.

The issuer's role is to communicate its risk appetite to the FI, along with the methods used by the issuer to stay within that appetite; the FI's role is to determine if the issuer's risk appetite is acceptable to the FI and to monitor the issuer's commitment, at a macro level, to staying within that appetite. In some cases, the FI may decide that it is not necessary for the FI to engage in on-chain monitoring for certain relationship types, e.g. a "mint account" or similar where the issuer permits a bank or large, listed multinational to engage directly in minting/burning for its own internal purposes. In other instances, the FI may need to engage in a substantial level of on-chain monitoring – for example, an issuer with a higher risk appetite may decide to provide minting/burning services to a smaller DASP in an unregulated jurisdiction in a high risk third country. The issuer may give the FI comfort that the relationship will be managed by the issuer through extensive on-chain monitoring of that DASP to the n-degree. The FI, if comfortable with such an arrangement, could then establish its own monitoring programme to compare on-chain activity to the n-degree, at a macro level, to assess whether the issuer remains within its own risk appetite. Alternatively, the issuer's risk appetite may be somewhere in the middle, with services offered to a reasonable number of established DASPs in regulated markets in low and medium risk countries, meeting certain standards that permit minimally invasive on-chain monitoring by the issuer that is then paralleled by the FI at a consolidated level.

As is the case in any relationship, an issuer that engages in higher risk relationships will be more expensive for the FI to manage, given the necessary allocation of resources to ensure the FI remains comfortable with the issuer's activity. In the extreme, this could include a requirement on behalf of the FI to receive full transparency on the underlying wallet addresses of the issuer's riskier clients, which would permit the FI to establish a tailored monitoring programme, leveraging blockchain analytics.

Irrespective of the issuer's client portfolio, FIs should expect the issuer to demonstrate capabilities for detecting changes in the risk profile of its clients, including risks associated with the origin and destination of funds, transactional behaviours indicative of layering or obfuscation such as chain-hopping, and abrupt changes in velocity or behavioural patterns. Such monitoring by the issuer is critical to mitigate the risks of money laundering, terrorist financing and sanctions evasion that could flow through the ecosystem and, ultimately, may implicate the FI in its role of facilitating access to the underlying fiat currency. Regardless, the FI should maintain qualified staff that understand the nuance of blockchain monitoring – vendor solutions are not a substitute for the resource necessary to undertake appropriate oversight, to be able to initiate and process RFIs, and to maintain the capacity to engage in technical discussions with the issuer to clarify unclear activity.

Ultimately, should the FI decide to establish its own risk-based, on-chain AAR process to monitor the issuer's on-chain transactions, as well as the issuer's on-chain risk exposure, this could complement the FI's traditional banking AAR. A reasonable, risk-based on-chain AAR should be established (and assessed) on the basis of the issuer's client base and the issuer's corresponding control framework, with the understanding that the ultimate responsibility for detecting, preventing, and reporting financial crimes related to the issuer's clients and stablecoin usage rests with the issuer.

In line with the risk-based approach, the focus should be proportionate. For example, for a regulated issuer that mints/burns to regulated clients in lower risk jurisdictions, the emphasis should be placed mainly on monitoring the FI's direct banking activity with the issuer (as noted in the previous section), and may be complemented with industry available reports and public sources on the stablecoin's general use and reputation, including on-chain data. Actual on-chain monitoring may be limited to ad hoc instances that may indicate the issuer is not operating in accordance with its stated risk appetite (e.g. triggered through adverse media). Alternately, higher risk issuers servicing higher risk clients will demand a more extensive on-chain AAR, and at a greater frequency, leveraging the full capabilities of blockchain analytics to ensure the risk is appropriately managed. Given that much of the issuer's activity will be on-chain, the FI may consider how best to incorporate on-chain monitoring into the existing enhanced due diligence process to gain a complete understanding of the issuer's activity and form a clear view on the issuer's risk profile. Where appropriate in higher risk scenarios, FIs may also consider reviewing the on-chain provenance and history of stablecoins prior to redemption into fiat, or the source of large fiat deposits used to mint stablecoins (and any relevant corresponding on-chain flows).

Conclusion

The provision of banking services to a fiat-backed stablecoin issuer presents a series of novel challenges to an FI in building and maintaining an appropriate financial crime risk management framework. However, risk-based foundational principles continue to apply in understanding the purpose and nature of the relationship with the issuer and the expected activity of the issuer through accounts provided by the FI. It is the FI that defines its own risk appetite, and thus it is the responsibility of the FI to understand the issuer's risk exposure and how it manages that risk effectively, and to determine if the issuer is a suitable customer for the FI and under what conditions. The approach for on-going monitoring of the relationship is an extension of that determination. The FI's financial crime risk management framework should be designed to evaluate whether the issuer continues to operate as agreed through fiat-based monitoring, and, as necessary, risk-based on-chain monitoring.