Swiss Banking

Multibanking

A Practice-Oriented Guidance on Due Diligence and Disclosure Duties

September 2025
SBA Leaflet

1 Purpose and scope of this fact sheet

This fact sheet contains legally non-binding explanations intended to support regulated financial inter-mediaries in the implementation and use of multibanking. It provides practice-oriented guidance on the following two key areas:

- **Due diligence duties** under the Anti-Money Laundering Act (AMLA)[1]
- **Duties to provide information** to authorities

This fact sheet does not cover any legal duties beyond the aspects mentioned above that may rise from other legal areas such as data protection (Federal Act on Data Protection), bank-client confidentiality (Banking Act), contractual obligations or operational risks. This fact sheet does not claim to cover all legal risks, nor does it contain any technical information on how to implement multibanking.

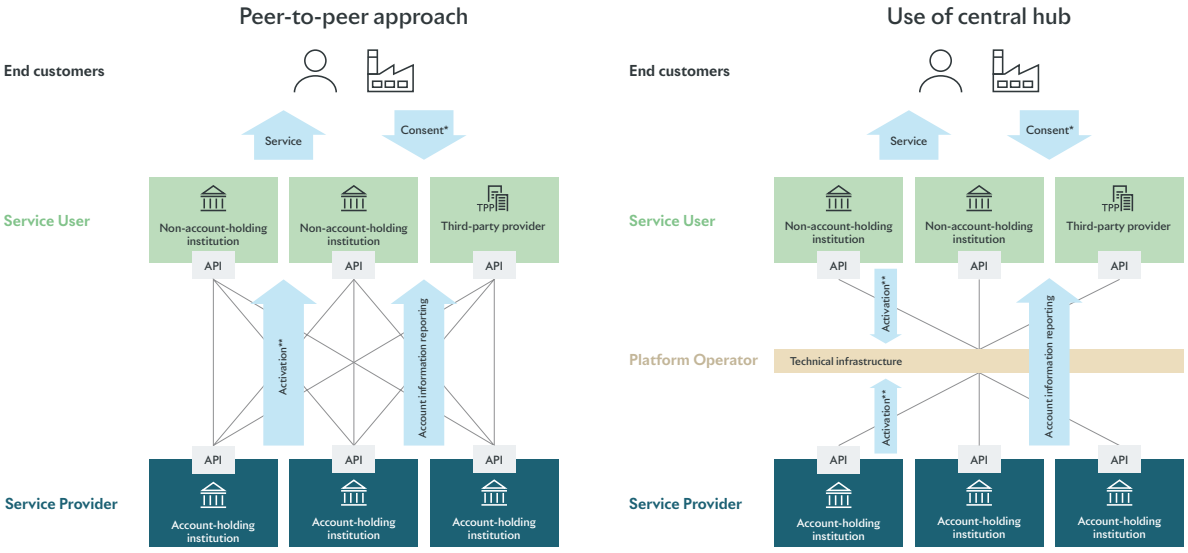
2 Terms and definitions

Multibanking
Multibanking is a use case of open banking that allows customers to manage accounts with multiple institutions on a single platform. It uses standardised application programming interfaces (APIs) to aggregate data from various account-holding institutions (banks) so it can be displayed on digital channels operated by other institutions or third-party providers. This can be implemented both directly between the institutions and other third-party providers and via a central technical infrastructure.

Roles
In principle, the following roles are defined:

- **End Customers:** customers of the bank or third-party provider using a multibanking service.
- **Service Provider:** In the case of multibanking, the Service Provider is always an account-holding institution that, at the request of its customers, makes the account data of its customers available for use by third parties (Service Users) in other environments.
- **Service User:** The service User takes data supplied by an account-holding institution (Service Provider) and makes it available in its own environment, e.g. e-banking or mobile banking. The Service User may be either a regulated financial institution or an unregulated third-party provider (TPP).
- **Platform Operator:** The Platform Operator normally provides a technical infrastructure (e.g. consent flow and standardised interfaces), sometimes together with additional services (e.g. standardised framework agreements for all participants), to connect Service Providers and Service Users.

1 SR 955.0 – Federal Act of 10 October 1997 on Combating Money Laundering and Terrorist Financing



* **Consent:** provided by customer to both account-holding institution (Service Provider) and non-account-holding institution (Service User)
** **API activation:** accounting-holding institution checked by platform operator (central hub) and/or non-account-holding institution
Information flow

Figure 1: The legal explanations apply in every case, regardless of the type of connection.

Regardless of the setups chosen in Figure 1, various questions arise from the perspective of a Service User that receives data from a Service Provider (account-holding institution) and acts as a regulated financial intermediary, particularly concerning its due diligence duties and its duties to provide information to authorities under the applicable anti-money laundering provisions. The explanations below apply to both peer-to-peer connections and connections via a central hub.

3 Selected legal issues for the Service User Bank

The core due diligence duties for a financial intermediary under the AMLA include the special due diligence duties set out in Art. 6 para. 2 AMLA, which form an essential part of the Act.[2] Particular attention must therefore be paid to these duties in the context of multibanking.

The financial intermediary must clarify both the economic background and the purpose of transactions and business relationships in the cases listed in Art. 6 para. 2 AMLA.

Given the frequency of use cases in practice, duties to provide information to authorities are also relevant in the context of multibanking.

3.1 Duty to monitor transactions

Art. 6 para. 2 AMLA requires the financial intermediary, among other things, to clarify the economic background and purpose of a transaction that carries a higher risk or appears unusual. This does not mean that all transactions need to be clarified in depth. Rather, the financial intermediary must remain vigilant and to follow up on any indications of suspicion.[3] In practice, this results in a de facto ongoing duty of transaction monitoring.[4] Art. 20 of the FINMA Anti-Money Laundering Ordinance (AMLO-FINMA) specifies the duty relating to transaction monitoring and requires the financial intermediary, among other things, to ensure effective monitoring of transactions.

3.2 Duty to clarify transactions and business relationships

When carrying out clarifications pursuant to Art. 6 para. 2 AMLA, financial intermediaries must, depending on the circumstances, take into account the information sources available to them in accordance with Art. 16 AMLO-FINMA.

3.3 Duty to provide information to authorities

In principle, an institution's duty to provide information to FINMA extends to all information within its control. The same generally applies to the duty to provide information and submit documents to other authorities, in particular to prosecution authorities.

---

2 See Doris Hutzler, in: Jürg-Beat Ackermann (ed.), Kommentar Kriminelles Vermögen – Kriminelle Organisationen: Einziehung – Kriminelle Organisation – Finanzierung des Terrorismus – Geldwäscherei, Volume II, Zurich/Basel/Geneva 2018, Art. 6 AMLA N 1.

3 Dispatch of 17 June 1996 on the Federal Act on Combating Money Laundering in the Financial Sector (Anti-Money Laundering Act, AMLA), 1127; see Cornelia Stengel, Transaktionsmonitoring mittels künstlicher Intelligenz, in: Jusletter, 5 June 2023, p. 11.

4 Thomas Müller/Matthias Lötscher, in: Peter Ch. Hsu/Daniel Flühmann (eds.), Basler Kommentar zum Geldwäschereigesetz, Basel 2021, Art. 6 AMLA N 37.

4 Possible approaches for the Service User Bank

The Service User Bank is responsible for determining how it takes into account and implements the above legal requirements and related explanations on an institution-specific basis in the context of multibanking.

4.1 Duty to monitor transactions

The financial intermediary is required to ensure effective monitoring of transactions. Such monitoring can be assumed to cover transactions carried out by the financial intermediary on behalf of its customers (including transactions between customers) as well as incoming transactions received on their behalf.

Based on this understanding, the Service User Bank is not required to include the available data on transactions carried out by the Service Provider Bank in its own transaction monitoring.

4.2 Duties to clarify transactions and business relationships

The legal requirements in the context of multibanking depend on the availability of data. The decisive factor is whether the Service User Bank has access to the Service Provider bank's data. Such access exists, for example, if the data is used for visualisations in its own e-banking or mobile banking system and stored on its own systems for this purpose, regardless of whether the Service User Bank uses the data for other purposes or how limited the group of people with access is.

Each institution must determine for itself what constitutes available data.

The Service User Bank must only include the available data from the Service Provider Bank in its own clarifications where its own business relationships require clarification under Art. 6 para. 2 AMLA. Each institution must define the scope of clarifications for itself.

In principle, situations may arise in which the data of the Service Provider Bank is not regarded as available the Service User Bank within the meaning of the AMLA. In such cases, the Service User Bank is not required to include these data in its clarifications of business relationships under Art. 6 para. 2 AMLA.

4.3 Duty to provide information to authorities

The scope of the duty to inform the authorities depends on the content of the order in each case. Banks are, however, only ever obliged to disclose information that is actually available to them. Where requests from authorities are unclear or unspecific (e.g. “further information that may be helpful to the authority”), whether in whole or in part, a bank may assume that such requests concern only the business relationships it manages.

Where a production order requires, inter alia, contractual or account-opening documents relating to a business relationship managed by the Service User Bank, it should be assumed that the Service User Bank’s multibanking agreement with its customers must also be submitted (see, for example, the list of “documents to be submitted” in the Swiss Conference of Prosecutors (SSK) recommendations for the production of electronic bank documents [three-stage model II]). In this case, there is no need to provide further information on the multibanking agreements, account balances or transaction data of Service Provider Banks unless explicitly requested by the authority issuing the order. Where the authority requests information on which data Service Provider Banks transmit to the Service User Bank under a multibanking agreement, such information must be provided if it is available to the Service User Bank.

Authorities can be expected to request account balances and transaction data from the original data source, i.e. the Service Provider Bank. This follows from the fact that the Service User Bank cannot guarantee the completeness of such data. Accordingly, production should take place at the primary source, namely the Service Provider Bank. The systems of the Service User Bank are designed exclusively for the automatic provision of its own data in line with the SSK recommendations (see above), and providing further information would involve a disproportionate effort. In addition, if a production order is directed only to the service user bank, the service provider bank would not be in a position to fulfil its due diligence duties under the AMLA, since in the absence of a production order it would lack any indication that assets may be of criminal origin and thus require clarification pursuant to Art. 6 para. 2 lit. b AMLA.

Swiss Bankers Association
Aeschenplatz 7
P.O. Box 4182
CH-4002 Basel
office@sba.ch
www.swissbanking.ch