Progress in combating money laundering

In recent years, banks and asset managers have been involved in numerous money laundering affairs in relation to major corruption scandals. With regard to combating money laundering, FINMA therefore focused its supervisory activities on how institutions deal with international money-laundering cases.

As part of its ongoing supervisory activities, FINMA examines whether institutions have learned from cases such as Petrobras, Odebrecht, 1MDB, Panama Papers, FIFA or PDVSA (see page 92). It also aims to harmonise the supervision by SROs.

In its supervisory work, FINMA has come across numerous examples of good conduct. This shows that many institutions have recently improved their money-laundering prevention processes significantly. However, FINMA still encounters negative cases. If necessary, FINMA takes enforcement measures.

Examples of good practice

- ✔ After conducting an enquiry in response to media reports into clients suspected of being involved in an international money-laundering case, a financial intermediary subsequently investigates whether the criteria for high-risk business relationships and transactions helped identify the suspicious relationships and transactions adequately or whether the criteria can be improved.
- ✔ After receiving a disclosure request from the Swiss Public Prosecutor's Office, a financial intermediary checks which other business relationships are connected to the relationship covered by the request. If the relevant conditions are fulfilled, they notify the Money Laundering Reporting Office Switzerland (MROS).
- ✔ A bank opens business accounts for a foreign group of companies and private accounts for its senior management staff. Neither the group nor the individuals have any connection to Switzerland. The authorised signatories of the operating companies make bonus payments directly to their private accounts. The bank looks into this structure and carries out an in-depth enquiry.
- ✔ A bank regularly carries out spot checks to determine whether the automated processes used for compliance work properly. In doing so, it identifies that due to an IT problem, certain updates to an external database have not been reconciled with its client base and it resolves the issue.

✔ The risk analysis carried out by a financial intermediary addresses the risks of terrorist financing.

Examples of bad practice

✘ A large financial intermediary has set up an automated system for checking against an external database in such a way that hits are only generated for identical names. A new client is entered into the bank's system with a double-barrelled name, while he is listed in the external database without a double-barrelled name. Because no hits are returned, the bank fails to identify that this person is a politically exposed person (PEP).

✘ A financial intermediary increases the required minimum assets so that a foreign PEP is managed as a client of the institution. Instead of parting ways with the PEPs with fewer assets, employees assume that numerous PEPs are no longer politically active and therefore the relationships no longer have to be managed as PEP relationships, and that for other relationships the PEP classification was unnecessary from the start. The PEP reclassifications are not scrutinised by supervisors.

✘ A client of a Swiss bank is a securities dealer from a Caribbean nation. The bank does not identify the beneficial owner, i.e. the client of the securities dealer, because its own client is subject to prudential supervision. Following a suspected case of insider trading, the bank is unable to provide the Swiss criminal authorities with the name of the beneficial owner.

✘ A bank has signed the Agreement on the Swiss Banks' Code of Conduct with regard to the Exercise of Due Diligence (CDB) and is thus subject to the corresponding private-law sanctions regime. Even in cases of serious breaches of the CBD, the bank fails to make an application by means of self-indictment.

Clear case law for reporting systems

The AMLA reporting system is of strategic importance for the reputation of Switzerland's financial centre. If criminals expect suspicious assets in Switzerland to be reported to the authorities, they are less likely to deposit assets resulting from criminal acts in the Swiss financial system. In a series of recent judgements, the Federal Administrative Court, the Federal

Criminal Court and the Federal Supreme Court clarified when a financial intermediary has to file a report. The most recent judgement by the Federal Supreme Court of 21 March 2018 (1B_433/2017, E. 4.9) concluded the following: "If a suspicion cannot be dispelled by carrying out background clarifications in accordance with Art. 6, para. 2 AMLA, it is to be regarded as reasonable."

According to the figures published by MROS in its 2017 annual report, the number of reports from financial-market intermediaries is rising continuously. There were twice as many reports in 2017 as in 2015. The high number of reports is not a result of minor cases: the average reported amount in 2017 was CHF 3.5 million. The high proportion of reports forwarded to the criminal authorities is also a sign that the quality of the reports is high. The most frequently reported predicate offence is bribery, followed by fraud. The first offence highlights how exposed the Swiss asset management centre is to money resulting from corruption abroad. The sharp rise in MROS reports points to a gradual cultural change in banks' reporting processes. Other financial-market areas are still reluctant to file reports. In 2017 for example, only four MROS reports were filed by lawyers in all of Switzerland.

Harmonisation of SRO supervision approaches

As part of its fourth country evaluation of Switzerland, the Financial Action Task Force (FATF) criticised the SROs' approach to supervision. In particular, the points criticised related to the differences between the supervisory approaches of the individual SROs as well as their sometimes insufficient or complete lack of focus on financial intermediary risks. Criticism was levelled, for example, at the disparate risk assessments of the various AMLA-relevant business activities in the parabanking sector and the lack of specific inherent risk criteria within a certain business activity (industry-specific criteria) in the supervisory approaches.

In light of this, FINMA is aiming to improve and harmonise the supervisory approaches of the individual SROs. After communicating the milestones and expectations in this regard to the SROs in 2017, the focus of work in 2018 was on materially revising and finalising the SROs' supervisory approaches. In some cases, FINMA monitored the individual SROs extremely closely throughout this process.

Focus of SRO supervision

This year, FINMA's focus in the area of SRO supervision was on SROs' resources for performing their core tasks with regard to onboarding new members, supervision as well as sanction measures and proceedings against members. In this respect, FINMA's on-site reviews in 2018 involved evaluating which resources the SROs dedicate to these core tasks.

The second focal point for FINMA was reporting. The reviews carried out focused on breaches of SRO members' obligation to clarify certain issues and the question of whether they led the SRO to investigate a potential breach of reporting requirements.