FINMA Risk Monitor 2023 – identification of nine significant risks relevant for financial service providers

20.12.2023

Key takeaways

- **Both liquidity and funding risks as well as outsourcing of significant functions have been newly added to the FINMA list of principal risks that financial service providers face; the other seven risks remain the same as last year.**
- **Cyber risks are among the most significant operational risks for financial institutions. As a first line of defense to prevent and mitigate cyberattacks, preventative access controls, monitoring procedures,and technical protections must be in place.**
- **Money-laundering risks in Switzerland remain high as an ever-growing number of new wealth management clients in Switzerland come from emerging-market countries where there is a significant threat of corruption. Money laundering risk analysis is a vital tool for the strategic management of banks and other financial intermediaries.**
- **The outsourcing of significant functions to third parties is a driver of operational risks at supervised institutions. The risks associated with significant outsourcing arrangements must adequately be identified, monitored, and controlled.**

Pestalozzi Rechtsanwälte AG
Feldeggstrasse 4
CH-8008 Zürich
T +41 44 217 91 11
zrh@pestalozzilaw.com

Pestalozzi Avocats SA
Cours de Rive 13
CH-1204 Genève
T +41 22 999 96 00
gva@pestalozzilaw.com

pestalozzilaw.com

Introduction

On 9 November 2023, the Swiss Financial Market Supervisory Authority ("FINMA") published its Risk Monitor 2023 in which FINMA identified nine significant risks relevant for financial service providers. Risks relating to liquidity and funding, as well as outsourcing of significant functions, have been newly added to the FINMA list of principal risks financial service providers face. The other seven risks remain the same as last year: interest rate risk; credit risks (both related to mortgages and other loans); market risk (credit spread risk); cyber risk; money laundering and sanctions as well as market access in Europe. With respect to longer-term trends and risks, this year FINMA is taking a closer look at artificial intelligence ("AI") in the Swiss financial market as the importance of AI has grown rapidly in many areas including the financial market industry. This legal update provides an overview on cyber, money laundering and outsourcing risks, notably those three risks that should be made a top priority not only for banks but for any FINMA supervised entity.

Cyber Risk

Cyber risks are among the most significant operational risks for financial institutions. Thus, FINMA is looking closely at the issue and has increased the intensity of its supervision in the past years as the financial sector in Switzerland has not been left unscathed by cyberattacks. Pursuant to the FINMA Risk Monitor 2023, 100 cyber reports have been submitted to FINMA over the past 12 months. With reference to cyberattacks, of utmost importance are the protection of individuals (i.e., creditors, investors, and insured persons) and the proper functioning of the financial markets directly or indirectly impacted by a cyberattack. Based on Art. 29 para. 2 of the Federal Act on the Swiss Financial Market Supervisory Authority ("FINMASA"), supervised entities must immediately report any incident that is of substantial importance to FINMA. Back in 2020, FINMA Guidance 05/2020 "Duty to report cyberattacks pursuant to Article 29 para. 2 FINMASA" was issued. The reports by supervised institutions to FINMA on cyberattacks confirm the trend that smaller institutions (category 5 institutions) are being attacked more frequently. Also, approximately 30% of insurers and approximately 20% of asset managers have been attacked over the past 12 months.

As a first line of defense to prevent and mitigate cyberattacks, preventative access controls, monitoring procedures, and technical protections must be in place. Most importantly, FINMA wants to see these measures, and these measures also need to be updated on a regular basis. Furthermore, supervised entities must have issued clear policies and procedures regarding how to react if and when cyberattacks occur.

Money Laundering Risk

The Swiss financial center is a leading global cross-border hub in wealth management; this means it is particularly exposed to money laundering risks. Money-laundering risk in Switzerland remains high as a significant number of new wealth management clients in Switzerland come from emerging-market countries, where there is a significant threat of corruption. Various global corruption and money-laundering cases show that the AML risks for financial institutions remain high. These risks are often increased by the use of complex structures. Therefore, compliance frameworks must keep pace with the risk appetite of a financial service provider. Also, risks in the crypto space are increasingly apparent, in particular with regard to crypto currencies. In the FINMA Risk Monitor 2023, FINMA once again established as a priority combating money laundering and terrorist financing. In the course of its supervisory work, FINMA identified weaknesses in transaction monitoring. To ensure effective reduction of money laundering risks, financial intermediaries must rigorously identity any such risks associated with business activities. Financial intermediaries are required to record, in their AML risk analyses, whether each of the individual criteria listed in the AMLO-FINMA are relevant to their business activity. In the course of its on-site supervisory reviews, FINMA determined that, in general, this requirement had either not been observed or had not been complied with adequately. Although risk analyses had been performed, they failed to go into sufficient detail. The money laundering risk analysis is an important tool for the strategic management of banks and other financial intermediaries. FINMA issued Guidance 05/23 "Money laundering risk analysis pursuant to Article 25 para. 2 AMLO-FINMA" on 24 August 2023. Finally, the increase in MROS report in the past years may indicate not only a cultural shift as well as better monitoring systems but also the continued existence of a number of significant risks.

Outsourcing

The outsourcing of significant functions to third parties is a driver of operational risks at supervised institutions. Pursuant to the FINMA Circular 2018/3, "outsourcing" -within the meaning of the circular- occurs when a supervised entity mandates a service provider to perform all or part of a function that is significant to the company’s business activities independently and on an ongoing basis. "Significant functions" are those that have a material effect on compliance with the aims and regulations of financial market legislation. Although supervised entities have long been using external service providers, pursuant to the FINMA Risk Monitor 2023, outsourcing has continued to increase in the recent years. The higher number of significant outsourcing not only increases the complexity for the individual institution, but also for the control of the respective service providers and their subcontractors. In the IT sector, especially, fewer service providers offering cloud services (Microsoft, Google, etc.) are performing key tasks, which results in new cluster risks for the financial market. In its Risk Monitor 2023, FINMA found that supervised entities have room for improvement in identifying their entire supply chain and the resulting risks. Further, in some cases, the risks associated with significant outsourcing arrangements have not been adequately identified, monitored, and controlled.

Conclusion

While new technologies facilitate improved efficiency in the financial sector, the danger of money laundering and the financing of terrorism are also heightened due to the potential of greater anonymity, along with the speed and cross-border nature of these transactions. Using cryptocurrencies, large amounts can be transferred from one electronic account to another in seconds, without the transactions' senders or recipients being identifiable. Cryptocurrencies too are often used in connection with cyberattacks or as a means of payment for illegal trading in the dark web. Also, money-laundering risks can be significant for fintech companies.

Author: Andrea Huber (Partner)

No legal or tax advice

This legal update provides a high-level overview and does not claim to be comprehensive. It does not represent legal or tax advice. If you have any questions relating to this legal update or would like to have advice concerning your particular circumstances, please get in touch with your contact at Pestalozzi Attorneys at Law Ltd. or one of the contact persons mentioned in this legal update.

© 2023 Pestalozzi Attorneys at Law Ltd. All rights reserved.

Andrea Huber



Partner
Attorney at law, LL.M.

Pestalozzi Attorneys at Law Ltd
Feldeggstrasse 4
8008 Zurich
Switzerland
T +41 44 217 92 41
andrea.huber@pestalozzilaw.com