Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

FINMA Guidance 02/2026

Digital fraud risks for banks and persons under Article 1*b* of the Banking Act

9 April 2026

Laupenstrasse 27, 3003 Bern, Tel. +41 (0)31 327 91 00, www.finma.ch

Contents

1 Introduction and terminology

Since the end of 2022, FINMA has observed a steady increase in cases of digital fraud at banks (hereinafter “institutions”). The latest technological developments, particularly advances in artificial intelligence and the digital transformation aimed at boosting efficiency through automation – such as online access to bank accounts or payment processing via instant payments, for example – are likely to further reinforce this trend.

Given the wide variety of forms these digital fraud cases take, it is not possible to formulate a definitive, universally applicable definition of digital fraud. Rather than a rigid definition, the term is therefore usually understood in functional terms: Digital fraud encompasses fraudulent acts in which digital technologies, information systems or electronic means of communication are used to deceive others with the aim of causing financial loss. Typical examples include identity fraud and identity theft, or situations where individuals are persuaded, through the fraudulent actions of third parties, to open bank accounts online that are subsequently misused for fraudulent purposes. The theft of login details and the opening of accounts online using forged identity documents also pose significant risks.[1]

Digital fraud risks can pose challenges to banks and persons under Article 1*b* of the Banking Act of 8 November 1934 (BA; SR *952.0*) in a number of ways: On the one hand, digital fraud risks can directly affect banks and their staff, for example through CEO fraud[2] and transfer fraud. On the other hand, bank clients can also fall victim to digital fraud, for example through real-time phishing.[3] In such situations, it is essential for institutions to identify fraud trends immediately and close any security gaps in order to prevent further instances of abuse and manipulation. This applies in particular where the digital infrastructure or the identity of the institutions is deliberately and systematically misused for fraudulent purposes. In such cases, a structural failure can not only result in significant legal risks for the institution, but also cause considerable damage to its reputation, which may have a lasting impact on client confidence. Digital fraud risks therefore constitute significant operational, legal and reputational risks, which the institution must take into account to a greater extent at all times by implementing appropriate organisational and technical measures.

At the end of 2025, FINMA conducted a survey on digital banking among 19 banks across various supervisory categories. In this guidance, it shares the

[1] In addition, there are, for example, client impersonation, various types of phishing, account takeovers and authorised push payments, as well as various forms of social engineering, in particular CEO fraud and wire fraud. Studies also show that generative AI is often used in cases where attempts at fraud have been uncovered in the European financial and payments sector.

[2] Scams based on supposedly urgent payment requests from senior executives.

[3] Scams in which attackers interactively obtain bank login details or authorisation codes in order to take control of accounts and make fraudulent payments.

findings it has obtained through this survey and its other supervisory activities. The aim is to raise awareness among banks and persons under Article 1*b* of the Banking Act of the risks of digital fraud, with a view to establishing effective defence measures.

2 Legal framework

Banks and persons under Article 1*b* of the Banking Act must provide for appropriate risk management within the scope of their business activities. Risk management must cover all business activities and be organised in such a way that all material risks can be identified, assessed, controlled and monitored. These risks also include operational risks, as well as legal and reputational risks. For banks and persons under Article 1*b* BA, this obligation to identify, limit and monitor their risks arises primarily from the organisational requirements pursuant to Article 1*a*, Article 1*b,* Article 3 para. 2 let. a and Article 3*c* BA in conjunction with Article 12 para. 2 and Article 14*e* of the Banking Ordinance of 30 April 2014 (BO; SR *952.02*). FINMA has laid down its supervisory practice in this regard in Circular 2023/1 “Operational risks and resilience – banks”. As regards money laundering prevention, the relevant duties in respect of due diligence arise in particular from Articles 3–6 of the Anti-Money Laundering Act of 10 October 1997 (AMLA; SR *955.0*) and Articles 13 ff. of the FINMA Anti-Money Laundering Ordinance of 3 June 2015 (AMLO-FINMA; SR *955.033.0*). Supervisory practice in the context of the digital provision of financial services was also set out in detail in FINMA Circular 2016/7 “Video and online identification”.

3 Findings and recommendations from the digital banking survey

The survey on digital banking reveals various shortcomings among the institutions surveyed in their handling of digital fraud risks. This highlights a particular need for concrete action regarding operational risk management in relation to digital fraud risks (including governance and risk management, and the detection of and response to such risks), as well as in dealing with cases of fraudulent use of accounts opened online and in the context of preventing money laundering.

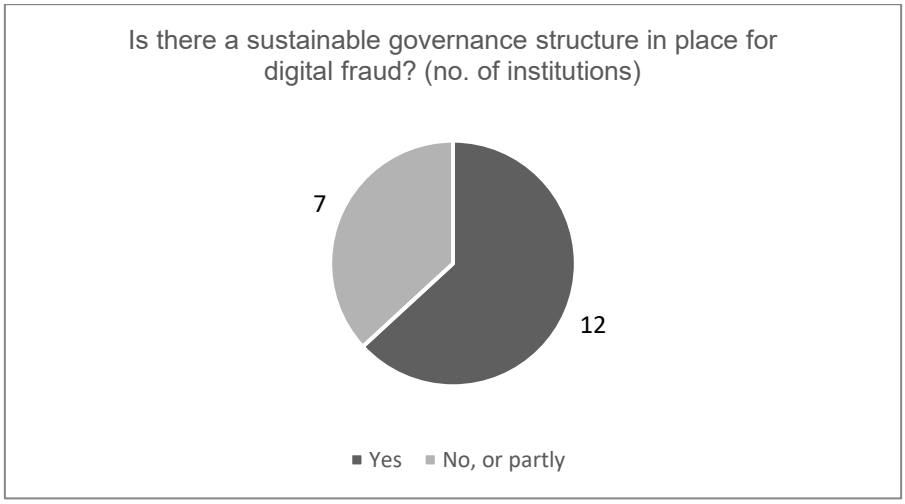
3.1 Operational risk management in relation to digital fraud risks

3.1.1 Governance and risk management in relation to digital fraud risks

Findings

The survey revealed that many institutions lack clear governance structures with regard to digital fraud risks. This is despite the fact that digital fraud on the Swiss financial market can result in significant losses for both clients and financial institutions. According to the Banking Ombudsman's 2024 annual report, fraud was the most common cause of the cases brought to its attention.[4]

Twelve out of 19 institutions stated in the survey that they have sustainable governance structures in place for digital fraud. It was found that these consist mainly of members holding two offices at the same time[5] – without clear allocations of tasks or responsibilities, and without clear and documented rules governing their powers.

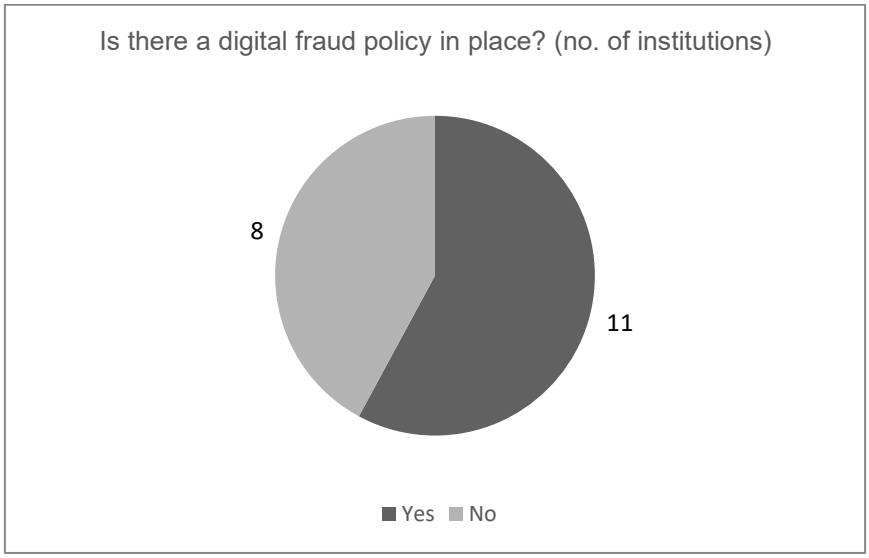


Furthermore, three of the institutions surveyed stated that they had no steering committee at all to deal with digital fraud risks. On the positive side, the results achieved by using interdisciplinary fraud desks to comprehensively manage requirements, controls and processes in the area of digital fraud risk management, with a clear reporting structure, are worthy of note.

[4] See Annual Report of the Swiss Banking Ombudsman 2024, page 8.

[5] For example, from Security Operations, Payments, Risk Management and IT.

Many of the institutions surveyed lack their own internal guidelines on how to deal with digital fraud risks. Instead, these issues are addressed through other guidelines (namely those relating to employee transactions, money laundering or information security), without these guidelines being aligned with one another. Consequently, eight of the 19 institutions (42%) do not have a digital fraud policy.



Furthermore, only around half of the institutions surveyed regularly include key figures relating to digital fraud cases in their reports to senior management.

Recommendations

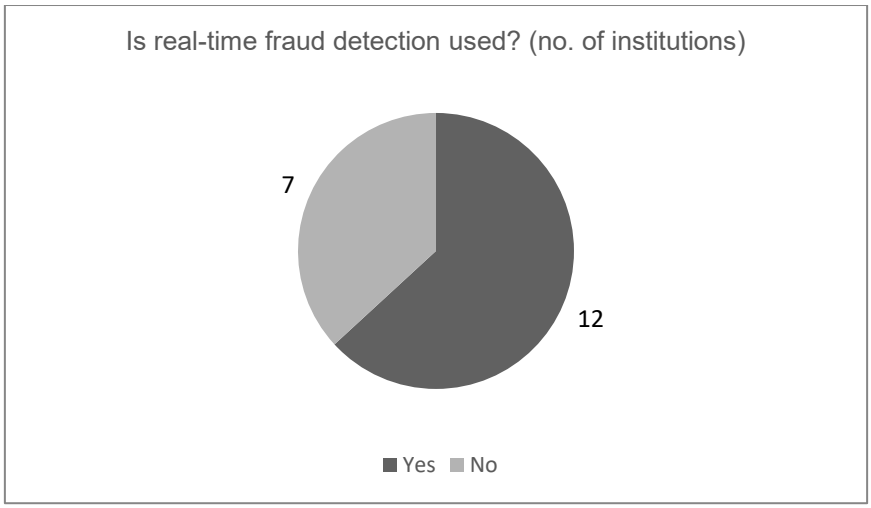
FINMA points out that digital fraud risks can pose significant risks to the institution, which must be comprehensively identified, assessed, managed and monitored by establishing internal responsibilities and procedures. In accordance with FINMA's supervisory practice, institutions must establish the necessary structures, guidelines, processes and controls within the framework of their governance and risk management to mitigate these operational risks.

3.1.2 Identifying and responding to digital fraud trends

Findings

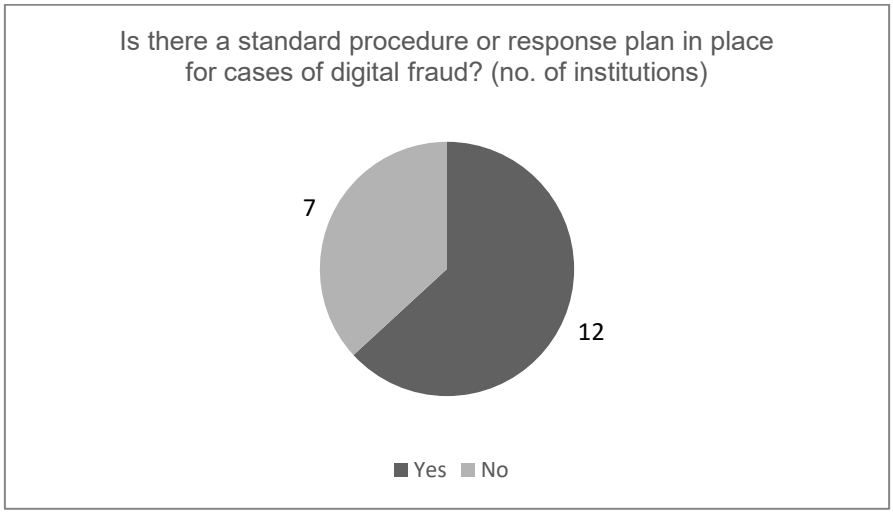
The survey revealed that 26% of the institutions surveyed have no processes in place for identifying and anticipating digital fraud trends (known as 'horizon scanning'). This means that these institutions are unable to proactively identify relevant fraud threats and scenarios affecting their digital services, and consequently cannot take appropriate precautions.

Furthermore, twelve out of 19 institutions use real-time fraud detection technologies.



Conversely, seven institutions stated that they either did not analyse indicators of ongoing digital fraud campaigns at all, or only did so manually or on a case-by-case basis. This makes it difficult to identify relevant patterns across multiple levels. Furthermore, due to their heavy reliance on service providers, not all institutions are able to update relevant detection rules in a timely manner, which jeopardises their ability to respond promptly to identified fraud campaigns or patterns.

The survey also revealed that there is room for improvement in the standardisation of response procedures and the relevant guidelines: Seven of the 19 institutions surveyed lack a standard procedure or response plans for cases of digital fraud.



Furthermore, only seven out of 19 institutions stated that they update their response plans at least once a year. The remaining institutions surveyed update their response plans only on an ad hoc basis, i.e. only after an incident has occurred. Generally speaking, most institutions do not set, measure or monitor response times in relation to reports of digital fraud. Only a few of the institutions surveyed offer 24/7 access to their reporting channels. Furthermore, very few institutions have specific channels for reporting fraud. Instead, they receive such reports via the general telephone helpline.

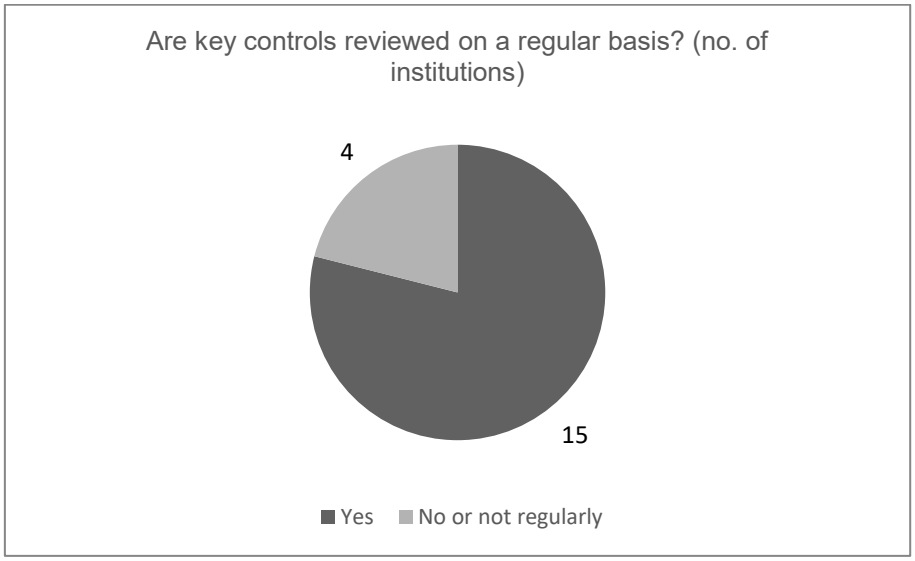
Recommendations

Effectively combating digital fraud risks requires proactive, timely, systematic and institution-wide detection, as well as the immediate implementation of appropriate countermeasures should an incident occur. Inadequate detection mechanisms and delayed response times can lead to an increase in the number or severity of fraud cases, the irretrievable loss of assets, and a failure to stop transactions related to money laundering in time.

3.1.3 Controls and effectiveness reviews of fraud prevention measures

Findings

Three of the institutions surveyed do not use any technical controls such as geo-blocking, IP risk rating or device fingerprinting to authenticate clients. Key controls, as an important tool for managing digital fraud risks, are absent at around 20% of the institutions surveyed, or their effectiveness is not regularly reviewed.



Some of the institutions surveyed stated that they do not provide further training for their staff on the risks associated with digital fraud. Although the other institutions do run training sessions, these often provide only general information about digital fraud risks rather than role-based training that takes into account the specific duties and risk profile of the participating staff members (e.g. client advisers). The methods used and the frequency of training sessions to raise awareness among staff and clients also vary considerably. Furthermore, not all of the institutions surveyed identify client segments that are particularly vulnerable or exposed to digital fraud risks.

Recommendations

As measures to prevent and combat digital fraud typically work at different levels, their integration and effectiveness must be reported in detail and regularly reviewed through appropriate controls.

Digital fraud risks are dynamic and constantly evolving. Regular staff training and raising client awareness are therefore important preventive measures for heightening awareness of potential fraud patterns.

3.2 Fraudulent use of accounts opened online

Findings

As part of its supervisory activities, FINMA has observed an increase in recent years in cases of fraud involving client accounts opened online. Criminal organisations are attempting to open bank accounts illegally using increasingly sophisticated technical means, through which illicit funds can be channelled. They are constantly developing and using increasingly sophisticated technical methods to circumvent regulatory controls during the account opening process.

When it comes to establishing client relationships online, fraudulent account opening (using forged identification documents or identity theft) poses a particular risk. This risk is exacerbated by the increased use of artificial intelligence, video manipulation software and deepfake technologies. Criminal organisations are making full use of the new technological possibilities, and manipulated videos or forged identity documents are becoming increasingly difficult to detect. However, the survey data do not provide clear evidence that there is an increased incidence of fraudulent activity when bank accounts are opened online. What is striking, however, is the increase in MROS reports relating to client accounts opened online. In addition to fraudulent account openings, there has been a rise in cases where individuals are tricked into opening accounts online using fraudulent means and by misrepresenting the facts, and then handing over access to

the accounts to criminal third parties once they have been opened. Furthermore, criminals use cybercrime methods (such as phishing attacks) to gain control of other people's accounts. The problem here is that accounts are often opened using valid identification documents, meaning that the account opening process is carried out in accordance with the applicable due diligence requirements. The actual fraudulent act then takes place in a subsequent step, when third parties gain control of the accounts.

Recommendations

Given the increased risks associated with opening accounts online, accompanying security measures are of paramount importance. These include, for example, the use of technical possibilities for detecting deepfakes and manipulated videos. In addition, as part of an appropriate risk management framework, staff must receive regular training on these developments (see also margin no. 8 of FINMA Circ. 16/7). Furthermore, the general risks associated with opening client relationships online and the risks of unauthorised account access should not be considered in isolation, but should be taken into account as part of a comprehensive digital fraud prevention strategy.

3.3 Money laundering prevention

Findings

The survey shows that the relative number of reports of suspected money laundering relating to (online) fraud, false identities, identity theft, unauthorised access to accounts, money mules and similar offences varies by a factor of up to 10 among the institutions surveyed. Furthermore, the proportion of internally generated reports that lead to MROS suspicious activity reports varies between 12 and 78%. Overall, the survey responses thus point to significant differences between institutions in the effectiveness of their anti-money laundering regulations, systems and processes when it comes to detecting fraudulent schemes.

According to the survey, the know your customer (KYC) information collected is generally rather limited. Furthermore, most institutions do not use the KYC information they collect for transaction monitoring at all, for example by applying different scenarios or limits. KYC information is generally only consulted during specific checks to verify its validity. In transaction monitoring, the thresholds above which routine transactions involving retail clients with low or normal risk are identified as transactions with increased risks are set relatively high at most of the institutions surveyed (CHF 100,000 or 200,000). This suggests that these are relatively unsophisticated systems, which identify transactions with increased risks primarily using fixed limits rather than specific scenarios. It is likely to be

correspondingly difficult for these institutions to identify cases of digital fraud as part of their transaction monitoring.

Recommendations

FINMA reminds institutions that their anti-money laundering regulations, as well as the systems and processes they use, must be sufficiently effective to detect cases of digital fraud and money muling as quickly as possible. In particular, transaction monitoring systems must be capable of identifying potential suspicious cases immediately.

4 Conclusion

Banks and persons under Article 1*b* of the Banking Act must establish appropriate governance and effective risk management systems to identify, mitigate and control digital fraud risks; this must cover all business activities and be organised in such a way that all material risks can be identified, assessed, managed and monitored. This also includes the risk of digital fraud when establishing client relationships online, particularly in relation to unauthorised account access. In order to monitor the significant legal and reputational risks associated with this effectively and to take preventive action, institutions require clear management tools and structures, processes and responsibilities, effective detection and response capabilities, a sophisticated transaction monitoring system for anti-money laundering purposes, and targeted tools for assessing the effectiveness of controls. In the event of a spate of fraud cases, the effectiveness of the measures in place to identify and prevent such incidents must be reviewed promptly and, if necessary, supplemented by additional measures. This may also include temporary restrictions on the provision of certain services that lead to such instances of digital fraud.