IOSCO'S STATEMENT ON RISING FRAUD TARGETING RETAIL INVESTOR ACCOUNTS AT MARKET INTERMEDIARIES

Introduction

The International Organization of Securities Commissions (IOSCO) is warning retail investors and market intermediaries that fraudulent schemes targeting retail investor accounts held at market intermediaries are on the rise and becoming more sophisticated.

Fraudulent actors are increasingly leveraging artificial intelligence (AI), social engineering, and digital channels to reach more investors, across more jurisdictions, and with greater impact than before. Such schemes have the potential to harm investors, weaken market integrity, and diminish investor confidence in financial markets.

The Statement details areas contributing to the rise in this type of fraud and shares lessons learned that can help reduce investor harm. It is intended to raise awareness of the increasing fraud risks and to share observations from IOSCO's work; it does not create new IOSCO standards. The practices described are illustrative and may be considered by market intermediaries if appropriate to their business and consistent with the laws and regulations of their jurisdiction.

A significant and growing risk

The findings from IOSCO's analysis point to a consensus among regulators and industry participants that fraud remains a significant and growing risk, including fraud schemes that involve the misuse, hacking or unauthorised access to the systems and accounts of regulated and legitimate intermediaries. Online and retail-facing intermediaries, in particular, reported increases.

Respondents indicated that incidents are becoming more complex and extend across borders. Industry respondents reported large-scale phishing campaigns and account takeover incidents affecting multiple firms, suggesting increasingly organized and coordinated threat activity. Regulators reported market manipulation schemes that generated substantial illicit profits through coordinated promotion and trading.

The retail investor segments most affected by this type of fraud include vulnerable investors, less sophisticated investors, self-directed online investors, and social media-active investors. Regulators also noted that online engagement, rather than demographic characteristics alone, is an important driver of exposure to fraud.

Origins of the growth

Regulators and market intermediaries pointed to several factors behind the rise in fraud, many of which they expect to persist:

- **AI is amplifying existing fraud**: AI is generally used to enhance and rapidly scale up existing fraud typologies rather than create entirely new ones. The most commonly reported uses include AI-generated phishing and social-engineering content, automated attacks such as bots coordinating account takeover attempts, the creation or enhancement of synthetic identities, and impersonation through deepfakes and voice cloning. AI can rapidly generate marketing content, fraudulent websites, forged documents, synthetic audio and video, and highly personalized communications, reducing the time, cost, and effort required to launch and scale fraud campaigns. Respondents identified AI-enabled fraud as the most significant emerging risk over the next 12 to 24 months, although its full impact remains difficult to assess.

- **Digital finance lowers barriers to execution**: Digital onboarding, instant payments, and the increasing involvement of crypto-assets can facilitate fraudulent schemes by lowering barriers to execution and complicating detection and recovery by intermediaries. Speed, irreversibility, and limited traceability are common characteristics of the payment and exit channels most commonly used, with bank transfers and crypto-asset channels most frequently reported.

- **Victims are increasingly deceived into authorizing the transactions themselves:** A growing proportion of fraud losses arise from scams in which victims authorize transactions after being manipulated or socially engineered. These schemes can be particularly difficult to detect because the activity may appear legitimate.

- **Fraud is becoming industrialized:** Schemes are increasingly supported by criminal networks that combine social engineering, digital platforms, AI-enabled tools, mule networks, and the rapid cross-border movement of funds. Some operate on a "fraud-as-a-service" model and, where cases involve overseas entities, foreign-hosted websites, or crypto-asset networks, identifying perpetrators and recovering assets is more difficult.

Common schemes to recognize

Fraudulent actors typically first gain access to a retail investor's account or credentials in a legitimate intermediary and then use that access to misappropriate assets. The most frequently observed techniques include:

- Impersonation of trusted individuals or organizations, such as regulators, law enforcement, investment advisers, market intermediaries, financial institutions, , particularly through the increasing use of AI-generated audio, video, and images, as well as fake or cloned websites and applications.

- Phishing, smishing, quishing, and vishing, where fraudulent actors pose as trusted entities by email, text message, or telephone to obtain credentials or other sensitive information, often by creating a false sense of urgency.

- Account takeover, which survey respondents identified as one of the most frequently observed attack vectors. It often results from social engineering, credential theft, or malware.

- Identity theft and synthetic identity onboarding, where fabricated identities combining real and fictitious information are used to evade standard onboarding and verification controls by licensed intermediaries.

Market intermediaries: steps to remain resilient

IOSCO recognises that many forms of fraud do not involve tampering with or hacking the systems of financial intermediaries and are beyond their reach. For the other categories, described above, IOSCO encourages market intermediaries to remain vigilant and to keep their fraud controls under review as fraudulent actors continuously adapt their methods.

Fraudulent actors most frequently target login and authentication, account opening and onboarding, changes to customer details or bank accounts, identity verification, transfer and withdrawal instructions, and interfaces with third-party systems. Online channels and call centres appear to be commonly affected.

Drawing on recent incidents, respondents identified the following lessons learned:

1. Phishing-resistant multi-factor authentication and enhanced identity verification remain critical for mitigating account takeover risk. Respondents found these controls most effective when applied consistently at critical points such as login, profile changes, and withdrawals.

2. Changes to customer details, banking information, and withdrawal instructions are a common point of attack. Enhanced verification, supported by customer notifications, callback verification, and cooling-off periods, can reduce this exposure.

3. Real-time monitoring and timely escalation can reduce losses and limit the impact of fraudulent activity. Behavioral analytics that combine transaction, contextual, and device-related indicators can help identify social engineering and customer-authorized transactions that may appear legitimate when viewed from a transaction-only perspective.

4. Effective prevention relies on a layered, risk-based approach that combines authentication, transaction monitoring, onboarding controls, and detection capabilities. Controls that depend primarily on customer vigilance tend to be less effective against sophisticated social-engineering attacks.

5. Clear escalation procedures, management oversight, and post-incident reviews help firms identify and close control gaps.

6. Many fraud controls rely on external providers. Understanding these dependencies, and maintaining fallback arrangements that have been tested, can strengthen operational resilience.

7. Where suitable, AI-assisted tools can support fraud detection, provided they are subject to human oversight and regularly tested against changing fraud techniques.

Investors: steps to protect against fraud

IOSCO urges retail investors to remain alert to the risk of fraud, particularly when investing online or engaging with investment content on social media and messaging platforms. Fraudulent communications can be convincing and increasingly use AI-generated content that is difficult to distinguish from genuine material. Investors are encouraged to consider the following:

1. Treating unsolicited calls, emails, text messages, QR codes, social media messages, and invitations to investment group chats with extreme caution, even where they appear to come from a known contact, a firm, a regulator, or a well-known person.

2. Checking official registration sources to confirm that any firm or investment representative they are dealing with is properly registered in their jurisdiction.

3. Contacting their firm only through contact details obtained independently, for example from the firm's official app or account statements, rather than those provided in a message, advertisement, or search result. Fraudsters may copy genuine firm names, logos, and registration details. Investors should therefore verify contact details, including URLs, to ensure they are dealing with legitimate channels and not fraudulent ones created by fraudsters.

4. Never sharing passwords, one-time codes, or other login details, and using the strongest authentication their firm offers, such as multi-factor authentication or passkeys.

5. Stopping, pausing, and taking time before transferring funds or securities, as a false sense of urgency is a common sign of fraud. Particular caution is warranted when asked to move money out of an investment account, to buy crypto-assets, or to invest in little-known or thinly-traded securities.

6. Before transferring funds or securities, discussing the proposed transaction with a trusted person, such as a family member, friend, financial professional, or legal adviser. A second opinion can help identify potential warning signs and reduce the risk of acting under pressure or in response to fraudulent communications.

7. Checking warnings issued by their national regulator and by IOSCO's International Securities & Commodities Alerts Network (I-SCAN), which allows anyone to check whether a company has been flagged by financial regulators.

8. Contacting their firm without delay through its official channels if they suspect fraud, and reporting the matter to their regulator and law enforcement. Funds can be moved quickly and may be difficult to recover once transferred.

The role of cooperation

Contemporary fraud schemes frequently span multiple products and jurisdictions, making timely information exchange and coordinated responses essential.

The respective roles of regulators and market intermediaries are complementary. Market intermediaries can identify and respond to account-level activity and operational vulnerabilities and help educate their clients about how to avoid frauds and scams, while regulators can identify market-wide patterns, coordinate information across firms and jurisdictions, issue guidance, disrupt unlawful activity, and take enforcement action. IOSCO members reported a combination of public warnings, investor education, guidance to firms, thematic reviews, enforcement actions, and disruptive measures such as website takedowns.

IOSCO encourages continued cooperation and information sharing among market intermediaries, regulators, law enforcement authorities, banks and payment providers, digital platforms, and technology providers, as consistent with applicable law. IOSCO will continue to support its members in addressing increasingly international and technologically enabled fraudulent schemes, including through its existing cross-border cooperation arrangements.