



Monetary Authority of Singapore

Guidelines on Anti-Scam Measures for Brokers



Contents

1	Introduction	3
2	Application of Guidelines	4
3	Definitions	5
4	Anti-Scam Measures	6
4.1	<i>Responsibilities of the Board and Senior Management</i>	6
4.2	<i>Login Controls</i>	6
4.3	<i>Trade Placement and Trade Execution Controls</i>	7
4.4	<i>Funds Withdrawal Controls</i>	8
4.5	<i>Ongoing Monitoring</i>	9
4.6	<i>Incident Handling</i>	10



1 Introduction

- 1.1 The Monetary Authority of Singapore (“MAS”) has observed a rise in scams targeting investors through capital market intermediaries, particularly brokers. Scam threats continue to evolve and have shifted over time across different parts of the financial system. Scammers have increasingly exploited vulnerabilities in digital channels, using impersonation and social engineering techniques to gain unauthorised access to customer accounts. Once access is obtained, scammers perform unauthorised activities, such as the trading of illiquid stocks, causing financial losses to victims. These activities erode customer trust and threaten the integrity of the financial system. It is therefore important that brokers adopt sound and responsive anti-scam risk management frameworks to protect their customers, and continue to strengthen their capabilities to detect, prevent and respond to scam risks in a timely manner.
- 1.2 These Guidelines on Anti-Scam Measures for Brokers (the "Guidelines") set out MAS’ supervisory expectations for anti-scam measures that retail brokers should implement to protect retail customers from unauthorised access to their trading accounts and from scam-related financial losses. Unless otherwise stated, references to “brokers” and “customers” in these Guidelines are references to retail brokers and their retail customers, respectively. MAS also strongly encourages all other brokers to adopt these measures proactively, where appropriate.
- 1.3 These Guidelines take effect on 30 June 2027. All retail brokers are however strongly encouraged to implement the anti-scam measures as early as practicable.



2 Application of Guidelines

- 2.1 In implementing these Guidelines, a broker should calibrate its anti-scam measures to the nature of its business, customer base, and overall risk profile. A broker should also ensure that its anti-scam measures remain effective and are regularly reviewed to keep pace with developments in the scams landscape and new scam typologies.
- 2.2 These Guidelines are not intended to be exhaustive or to override any legislative provisions. They should be read in conjunction with the provisions of the Securities and Futures Act 2001 (“SFA”), the relevant subsidiary legislation made thereunder, as well as written directions, notices, codes and other guidelines that MAS may issue from time to time pursuant to the relevant legislation and subsidiary legislation. The Guidelines do not affect and should not be regarded as a statement of the standard of care owed by brokers to their customers.
- 2.3 A broker should be able to demonstrate to MAS its observance of the expectations in these Guidelines. Where MAS is not satisfied with the broker’s observance of the expectations in these Guidelines, MAS may require the broker to take additional measures to address the deficiencies noted. MAS may also take non-observance into account in its assessment of the broker, considering the severity of the deficiencies noted, the broker’s track record in internal controls and risk management, and the circumstances of the case.
- 2.4 A broker should maintain sufficient documentation to demonstrate observance with these Guidelines and provide such documentation to MAS upon request.
- 2.5 MAS expects all brokers to remain vigilant and responsive to emerging risks and to continuously review and enhance their controls. MAS may review and update these Guidelines as necessary to reflect developments in the scams landscape.



3 Definitions

3.1 In these Guidelines, unless the context otherwise requires:

"account contact" means the contact information that a customer has provided to the broker, including a customer's registered phone number or email address, for the broker to send notification alerts for transactions, logins to the customer's account on a new device or browser, and changes in account details;

"direct messaging channel" means Short Messaging Service ("SMS") or other equivalent messaging services that deliver messages directly to the customer's registered mobile number;

"retail broker" means a broker that provides dealing services to retail customers;

"trading account" means any account maintained by a customer with a broker for the purpose of trading in capital markets products; and

"unauthorised transaction" means any transaction initiated by any person without the actual or imputed knowledge and implied or express consent of a customer.

4 Anti-Scam Measures

4.1 Responsibilities of the Board and Senior Management

- 4.1.1 The Board and Senior Management play a critical role in establishing a sound governance and risk management framework for managing scam risks, and ensuring that such risks are appropriately assessed, monitored and mitigated as part of the broker's overall risk management framework.
- 4.1.2 The Board and Senior Management should establish a robust governance framework for the oversight of scam risk and the fair treatment of customers. This should include, amongst others, an effective incident management process to enable a prompt and coordinated response to scam attacks targeting customers.
- 4.1.3 The Board and Senior Management should implement, and ensure compliance with, effective written policies and procedures on anti-scam measures to protect customers from unauthorised access to their trading accounts and from scam-related financial losses.
- 4.1.4 The policies and procedures should amongst others, include:
 - (a) the handling of incidents relating to unauthorised access to customers' trading accounts. Such procedures should be designed to enable the immediate containment of threats and an efficient response to minimise customer losses; and
 - (b) the handling of customer losses arising from fraudulent activities. Such procedures should be designed to ensure fair, consistent and transparent outcomes for customers, including clear principles for assessing claims relating to unauthorised transactions.

4.2 Login Controls

- 4.2.1 Brokers should implement two-factor authentication for all customer logins to trading accounts.¹ Such authentication should include at least one factor that is phishing-resistant², e.g. biometrics or device-bound cryptographic keys, to mitigate the risk of unauthorised access arising from compromised credentials.
- 4.2.2 Brokers should provide real-time notification alerts to customers whenever there is a login to their trading account from a new device or browser. Where there is a login to a customer's account from a new device or browser:
 - (a) the notification alert should be sent to the customer's account contact. Where the customer has provided more than one account contact, the notification alert should be sent to every account contact selected by the customer to receive such notifications;

¹ MAS had issued a set of [Frequently Asked Questions on Two-Factor Authentication for Online Financial Services Platforms](#), which should be read together with the expectations set out in paragraph 4.2.1.

² One-time passwords, whether delivered via hardware tokens, authenticator applications, or SMS, remain susceptible to phishing and are not considered phishing-resistant.

- (b) the notification alert should, by default, be conveyed to the customer by way of a direct messaging channel. Brokers may allow customers to subsequently change their preferred notification channel, provided that they clearly disclose the associated risks of the change and obtain the customers' explicit acknowledgement of the relevant risk disclosures before the change takes effect;
- (c) the notification alert should contain sufficient information to enable the customer to identify the login activity, including details such as geolocation where available, and should include a reminder for the customer to contact the broker if the login was not performed by the customer; and
- (d) the notification alert should not contain clickable links or Quick Response ("QR") codes via any direct messaging channel or email, unless:
 - (i) the link or QR code contains only information for the customer and does not lead to a website where the customer is required to provide his login credentials or perform any transactions, or a platform where the customer is able to download and install applications; and
 - (ii) the customer is expecting to receive the communication from the broker.

4.2.3 Brokers should implement controls to manage concurrent access to customers' trading accounts. As a default, a customer should be limited to one active trading session at any one time. Where a customer has a genuine operational need for additional concurrent sessions, brokers may permit a reasonable number of such sessions, subject to appropriate safeguards³ and where justified by the customer's needs. Brokers should also implement automatic session timeouts after a period of inactivity to reduce the risk of prolonged unauthorised access through a hijacked session.

4.3 Trade Placement and Execution Controls

- 4.3.1 Timely notification of trade activity is critical to enable customers to promptly detect unauthorised transactions and take appropriate actions. Brokers should, by default, provide customers with notification alerts for all trades placed and executed on their trading accounts.
- 4.3.2 Such notification alerts should be provided on a real-time basis, separately at the point of trade placement and trade execution, and should fulfil the following criteria:
 - (a) the notification alert should, by default, be conveyed to the customer by way of a direct messaging channel. Brokers may allow customers to subsequently change their preferred notification channel, provided that they clearly disclose the associated risks of the change and obtain the customers' explicit acknowledgement of the relevant risk disclosures before the change takes effect;

³ Examples of such safeguards include (i) implementing a maximum number of concurrent sessions allowed, even for customers with genuine operational needs, and (ii) conducting periodic review of customers who have been granted multiple concurrent sessions to ensure the justification remains valid.



- (b) the notification alert should contain sufficient information to enable the customer to identify the transaction, for example, security name, order price or executed price, order quantity, order type, and timestamp of the transaction; and
- (c) the notification alert should not contain clickable links or QR codes via direct messaging channel or email unless:
 - (i) the link or QR code contains only information for the customer and does not lead to a website where the customer is required to provide his login credentials or performs any transactions, or a platform where the customer is able to download and install applications; and
 - (ii) the customer is expecting to receive the communication from the broker.

4.3.3 Brokers may allow customers to subsequently adjust their notification threshold for trades placed and executed on their trading accounts. Where such adjustments may result in notification alerts not being provided for certain trades, brokers should clearly disclose the associated risks of the change and obtain the customers' explicit acknowledgement of the relevant risk disclosures before the change takes effect. A notification should be sent to the customers' account contact by way of direct messaging channel whenever the notification threshold is changed.

4.4 Funds Withdrawal Controls

4.4.1 To mitigate the risk of unauthorised withdrawals and misuse of trading accounts, brokers should implement controls to ensure that funds withdrawals are authorised by, and made only to, bank accounts belonging to the customer. In this regard, brokers should verify that any bank account designated for withdrawal belongs to the customer. Such verification should be supported by appropriate due diligence measures, including obtaining supporting documentation, such as bank statements containing the customer's details.

4.4.2 Brokers should provide customers with real-time notification alerts for all withdrawals of funds. Such notification alerts should fulfil the following criteria:

- (a) the notification alert should, by default, be conveyed to the customer by way of a direct messaging channel. Brokers may allow customers to subsequently change their preferred notification channel, provided that they clearly disclose the associated risks of the change and obtain the customers' explicit acknowledgement of the relevant risk disclosures before the change takes effect;
- (b) the notification alert should contain sufficient information to enable the customer to identify the transaction, for example, the withdrawal amount, timestamp, and recipient account details; and
- (c) the notification alert should not contain clickable links or QR codes via direct messaging channel or email unless:
 - (i) the link or QR code contains only information for the customer and does not lead

to a website where the customer is required to provide his login credentials or performs any transactions, or a platform where the customer is able to download and install applications; and

- (ii) the customer is expecting to receive the communication from the broker.

4.5 Ongoing Monitoring and Notification for Suspicious Activities and Account Changes

- 4.5.1 To enable early detection of potential fraud and timely intervention, brokers should implement systems and processes to continuously monitor for suspicious account and trading activities. Such monitoring processes should be adequately designed, implemented and maintained to provide effective protection for customers and to mitigate the risks to the integrity and reputation of the financial system.
- 4.5.2 Brokers should adopt a risk-based approach in designing and implementing their monitoring processes, having regard to the nature, size and complexity of their business activities, as well as the profile of scam risks to which they are exposed. Brokers should ensure that their monitoring systems and processes are appropriately calibrated to the level of risk and capable of detecting suspicious account and trading activities on an ongoing basis. Such monitoring processes should include, as appropriate:
 - (a) monitoring for phishing campaigns and identifying fictitious or fraudulent websites and mobile applications that may target the broker's customers;
 - (b) detection of suspicious internet protocol addresses, device IDs or other indicators that may be associated with unauthorised access or potential scam activity;
 - (c) analysis of trends and patterns in customer behaviour to identify suspicious activities, including unusual changes to customer information, abnormal login patterns, and irregular trading behaviour that may indicate account compromise;
 - (d) enhanced monitoring for higher-risk transactions or activities, including large trades originating from non-resident jurisdictions or other indicators of potential account compromise; and
 - (e) monitoring for emerging trends and new modus operandi used by scammers and money mules.
- 4.5.3 Where changes are made to a customer's contact information, including contact number or email address, the broker should provide notification alerts to the customer's existing account contact prior to the change taking effect, to enable the customer to detect and prevent unauthorised modifications. Such notifications should fulfil the following criteria:
 - (a) the notification alert should contain sufficient information to enable the customer to identify the change in account details, and should include prominent and clear instructions directing the customer to contact the broker immediately if the change was unauthorised;

- (b) the notification alert should contain the broker's fraud reporting contact details for urgent assistance; and
- (c) the notification alert should not contain clickable links or QR codes via direct messaging channel or email unless:
 - (i) the link or QR code contains only information for the customer and does not lead to a website where the customer is required to provide his login credentials or performs any transactions, or a platform where the customer is able to download and install applications; and
 - (ii) the customer is expecting to receive the communication from the broker.

4.5.4 Brokers should ensure that the alerts generated from such monitoring are reviewed and acted upon in a timely manner. In particular, brokers should investigate suspicious activities and take appropriate intervention measures, including restricting account access or transactions where necessary, to prevent or mitigate potential customer losses.

4.6 Incident Handling

4.6.1 To limit and prevent further losses arising from unauthorised access and fraudulent activities, brokers should establish an effective incident handling framework. Such a framework should include accessible reporting channels, effective account restriction capabilities to promptly restrict compromised trading accounts, and clear procedures and policies for handling incidents of unauthorised access and customer losses arising from fraudulent activities. The framework should be robust and capable of enabling an immediate and coordinated response to contain risks and minimise customer harm.

4.6.2 Brokers should provide customers with easily accessible reporting channels to report unauthorised or erroneous transactions. Such reporting channels should, at a minimum, be available throughout trading hours, and be capable of enabling timely reporting and intervention. In particular, the reporting channels should fulfil the following criteria:

- (a) the reporting channel should include at least one manned phone line, monitored email address, or online portal that is capable of enabling a prompt response, to ensure that customers are able to seek timely assistance;
- (b) any person who makes a report through the reporting channel should receive written acknowledgement of their report by way of SMS, email, or in-application notification, confirming that their case is being investigated; and
- (c) the broker should not charge a fee to any person who makes a report through the reporting channel.

4.6.3 Brokers should treat all cases involving potential fraud or unauthorised access as a priority, with timely responses and prompt assistance provided to customers throughout the resolution process.



- 4.6.4 Brokers should have the capability to immediately restrict or freeze compromised trading accounts upon reporting by customers or upon detection of fraudulent activities, so as to prevent further unauthorised transactions and protect customer funds. A broker should designate dedicated personnel to act as a single point of contact for affected customers, to follow up on the status and progress of investigations throughout the resolution process.
- 4.6.5 Brokers should provide customers with a self-service account restriction feature on their platform and mobile applications. The feature should enable customers to immediately restrict specified functions of their trading accounts and should offer **both** of the following restriction options:

Option 1: Full Restriction (Default option)

Full Restriction is intended to secure the account by preventing all customer-initiated access and transactions until the broker has verified the customer's identity and is satisfied that it is appropriate to restore access. Upon activation, the broker should immediately:

- (a) suspend all existing login sessions and disable subsequent logins;
- (b) disable changes to account information and settings;
- (c) prevent the placement of new orders;
- (d) cancel all existing unfulfilled orders;
- (e) disable fund withdrawals; and
- (f) take any other measures as necessary to secure the customer's account.

Option 2: Limited Restriction

Limited Restriction is intended to allow the customer to manage existing positions while preventing new risk-taking and limiting account activity to the reduction or closure of those positions. Upon activation, the broker should immediately:

- (a) suspend all other active login sessions, other than the session used to activate the restriction;
- (b) disable changes to account information and settings;
- (c) prevent the placement of new orders that would establish new positions or increase the customer's exposure;
- (d) cancel all existing unfulfilled orders;
- (e) disable fund withdrawals; and
- (f) take any other measures as necessary to secure the customer's account.



For the avoidance of doubt, subsequent account logins may be permitted under this option, but any new transactions should be limited solely for the purposes of reducing or closing existing positions.⁴

- 4.6.6 The self-service account restriction feature should be easily accessible on the broker's platform and mobile application, so that customers can take immediate action to secure their account if required. Brokers should educate their customers on the purpose and implications of activating each restriction option, including the features that will be restricted and those that will remain available, before customers activate the relevant option.

⁴ Where customers are permitted to reduce or close existing positions, brokers should consider implementing appropriate complementary controls to guard against unauthorised sales at prices that are inconsistent with prevailing market prices to prevent customer losses. For example, by restricting such transactions to limit orders placed within pre-defined price collars.