



GENERAL RULEBOOK (GEN)

*In this attachment underlining indicates new text and striking through indicates deleted text.

3. MANAGEMENT, SYSTEMS AND CONTROLS

...

3.3 Systems and controls

...

Fraud

3.3.38 An Authorised Person must establish and maintain effective systems and controls to:

- (1) deter and prevent suspected fraud against the Authorised Person and its Customers; and
- (2) report suspected fraud and other Financial Crimes to the relevant authorities.

3.3.39 An Authorised Person must ensure that the systems and controls established and maintained in accordance with Rule 3.3.38:

- (1) enable it to identify, assess, monitor and manage Financial Crime risks, including Money Laundering Risk; and
- (2) are comprehensive and proportionate to the nature, scale and complexity of its activities.

3.3.40 In Rule 3.3.39(1), "Money Laundering Risk" is the risk that an Authorised Person may be used to further money laundering. In identifying its Financial Crime risks and Money Laundering Risk and establishing the necessary systems and controls, an Authorised Person should consider a range of factors, including:

- (1) its Customer, product and activity profiles;
- (2) its distribution channels;
- (3) the complexity and volume of its Transactions;
- (4) its processes and systems; and
- (5) its operating environment.

Guidance

Considering the evolving nature of Financial Crime, and the methods used to undertake it, an Authorised Person should apply best practice when establishing the systems and controls required under Rule 3.3.38. Such practices may include, but are not limited to, incorporating secure authentication, biometrics and the monitoring of customer behaviour metrics into anti-fraud and anti-Financial Crime systems and controls.

...