

Escalation and Identifying Potential Fraud



Document Details

Creation Date	July 2022
Issuer	Regulatory Anti-Fraud Compliance
Training Owner	Salvatore Bono, Antonios Poutnidis
Contacts	GG CH Anti-Fraud
Target Audience	Global Bank wide

Summary and key points

- **Escalate** any potential fraud or suspicious activity immediately.
- These include unusual incidents or concerns that pose/may pose significant risks. It could lead to financial loss for Credit Suisse/our clients or could cause other significant, non-financial, or reputational harm to our clients, personnel, Credit Suisse, and the integrity of the markets.

Escalation channels

- Your primary contact is your line manager (except when it is inappropriate to do so, e.g., your line manager may be involved in the incident/has failed to address it appropriately) or other appropriate management/senior management
- Compliance, Human Resources, General Counsel
- The Credit Suisse Integrity Hotline (phone) or Integrity Line (web) (where anonymous reporting is available, if permitted by law)

Internal fraud controls

- **Segregation of duties**
A second person should approve/authorize any transaction or process to prevent domination of controls, manual overrides, or collusion between Bank personnel.
- **Call-back verification**
Use to authenticate a request for client data (i.e., statements) or transfer of assets (i.e., wires, credit,

securities) by calling the telephone number of record to verify the identity of the requesting party and the legitimacy of the request.

- **Block leave**
To mitigate the potential risk of internal fraud, designated sensitive personnel must take 10 consecutive business days within a calendar year. In doing so, personnel must not perform duties relating to their role, access any Bank premises for business purposes, or use Bank systems.

External Fraud risks

The Bank and its personnel are vulnerable to external fraud risks, such as:

- Vendor and supplier fraud
- Financial statement fraud
- Payment fraud
- Investment fraud
- Cyber fraud
- Identity theft
- Credit Suisse brand misuse

Anti-Fraud Global Minimum Standards

Credit Suisse introduced the [Anti-Fraud Global Minimum Standards \(AFGMS\)](#) in 2021 to tackle internal and external fraud across all regions. In order to ensure adherence to the AFGMS, it is important to be familiar with the standards, e.g. [while working on Change Initiatives](#).

Other resources

- [Escalation Policy \(GP-00012\)](#)

- [Anti-Fraud Policy \(GP-00298\)](#)
- [Incident Collation Policy \(GP-00260\)](#)
- [US Cross Border Policy \(P-00025\)](#)
- [FATCA Policy \(GP-00085\)](#)
- [Disciplinary Policy \(GP-01058\)](#)
- [Global Block Leave Policy \(GP-00387\)](#)
- [Identity Theft Red Flags Supplement \(GP-00298 S-03\)](#)
- [Credit Suisse Integrity Lines \(phone and web\)](#)
- [Anti-Fraud Global Minimum Standards](#)