

# Escalation and Identifying Potential Fraud



## Document Details

Creation Date	April 2021
Issuer	Escalation: Global Conduct Risk/Global Investigations Fraud: Anti-Fraud
Training Owner	Alexandria Nguyen
Contacts	<a href="#">GG Conduct Risk</a> <a href="#">GG Anti-Fraud Americas</a>
Target Audience	Global Bank wide

## Summary and key points

- **Escalate** any potential fraud or suspicious activity immediately.
- Any incidents or concerns should be **escalated freely** and **without threat of retaliation**. All contacts and investigations are **treated as confidentially as possible**, subject to applicable laws and regulations.

## Escalation of unusual incidents or concerns

- **What?**  
Escalate unusual incidents or concerns that pose/may pose significant risks. These include unusual incidents or concerns that 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.
- **When?**  
Escalate without delay and in an effective manner. Early recognition and resolution of unusual incidents or concerns is key to mitigating risks.
- **How?**  
To the extent permitted by applicable laws and regulations, you may choose to remain anonymous when escalating an unusual incident or concern via the Credit Suisse Integrity Lines (phone and web).

## 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.

## Other resources

- [Escalation Policy \(GP-00012\)](#)
- [Anti-Fraud Policy](#)
- [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 \(phone and web\)](#)
- [Cultural values \[IMPACT\]](#)