

# Escalation e individuazione di potenziali frodi



## Dettagli del documento

Data di creazione	Luglio 2022
Emittente	Regulatory Anti-Fraud Compliance
Titolare della formazione	Salvatore Bono, Antonios Poutnidis
Contatti	GG CH Anti-Fraud
Pubblico destinatario	Global Bank wide

## Riepilogo dei punti chiave

- **Segnalare** immediatamente potenziali frodi o attività sospette.
- Tra di esse figurano gli eventi insoliti o i sospetti che comportano/potrebbero comportare rischi significativi. Potrebbero conseguire perdite patrimoniali per Credit Suisse/i nostri clienti o altri danni significativi, non finanziari o di reputazione, per i nostri clienti, collaboratori, Credit Suisse e l'integrità dei mercati.

## Canali di escalation

- Il vostro contatto principale è il responsabile di linea (eccetto quando è inopportuno farlo, p. es. può essere coinvolto nell'evento/ha omesso di affrontarlo in maniera appropriata) o un altro rappresentante del management/senior management competente
- Compliance, Human Resources, General Counsel
- La Integrity Hotline (linea telefonica) o la Integrity Line (pagina web) di Credit Suisse (che consentono la segnalazione anonima ove previsto dalla legge)

## Controlli per le frodi interne

- **Separazione dei ruoli**  
Una seconda persona deve approvare/autorizzare una transazione o un processo per impedire il dominio di un singolo sui

controlli, il superamento manuale dei controlli o la collusione tra il personale della banca.

- **Chiamate di verifica**  
Utilizzate per autenticare le richieste di dati dei clienti (p. es. estratti conto) o i trasferimenti di patrimonio (p. es. bonifici, credito, titoli) contattando il numero telefonico registrato per verificare l'identità del richiedente e la legittimità della richiesta.
- **Congedo obbligatorio ininterrotto**  
Per mitigare il rischio potenziale di frode interna, il personale sensibile designato deve usufruire di 10 giorni lavorativi consecutivi di congedo per ogni anno solare, in cui non è consentito svolgere compiti connessi al proprio ruolo, accedere ai locali della banca per scopi aziendali né utilizzarne i sistemi.

## Rischi di frodi esterne

La banca e il suo personale sono esposti a rischi di frode esterna, come per esempio:

- frodi di venditori e fornitori;
- frodi di bilancio;
- frodi nei pagamenti;
- frodi d'investimento;
- frodi informatiche;
- furto di identità;
- uso improprio del marchio Credit Suisse.

## Standard minimi globali antifrode

Nel 2021 Credit Suisse ha introdotto gli standard minimi globali antifrode

(AFGMS) per contrastare le frodi interne ed esterne in tutte le regioni. Al fine di garantire la conformità agli AFGMS, è importante familiarizzare con gli standard, p. es. quando si lavora alle Iniziative di cambiamento.

## Altre risorse

- Direttiva Escalation (GP-00012)
- Direttiva Prevenzione di frodi (GP-00298)
- Direttiva Operational Risk Incident Management and Collation (GP-00260)
- Direttiva per le attività di Private Banking transfrontaliere con gli Stati Uniti (P-00025)
- Direttiva Regimi di dichiarazione fiscale FATCA & SAI (GP-00085)
- Direttiva Rischio di condotta (GP-01058)
- Direttiva Congedo obbligatorio ininterrotto (GP-00387)
- Identity Theft "Red Flags" and associated detection, identification, escalation and reporting requirements supplement to Anti-Fraud (GP-00298-S-03)
- Credit Suisse Integrity Lines (phone and web)
- Standard minimi globali antifrode