

Procédure de remontée des incidents par la voie hiérarchique et identification de potentielles fraudes



Détails du document

Date de création	Juillet 2022
Émetteur	Regulatory Anti-Fraud Compliance
Propriétaire de la formation	Salvatore Bono, Antonios Poutnidis
Contacts	GG CH Anti-Fraud
Public cible	Banque entière, au niveau mondial

Récapitulatif et principaux points

- **Remonter** immédiatement toute fraude éventuelle ou activité suspecte.
- Cela comprend les événements sortant de l'ordinaire ou les préoccupations qui engendrent ou sont susceptibles d'engendrer des risques importants. Ces événements et préoccupations pourraient entraîner un dommage économique pour le Credit Suisse/nos clients ou pourraient causer d'autres préjudices importants, non financiers ou liés à la réputation, à nos clients, à nos collaborateurs, au Credit Suisse et à l'intégrité des marchés.

Canaux de transmission

- Votre interlocuteur principal est votre supérieur hiérarchique (sauf s'il est inapproprié de le faire intervenir, p. ex. parce qu'il est peut-être impliqué dans l'événement/n'a pas traité l'événement de manière adéquate) ou d'autres membres compétents de la direction ou du senior management
- Compliance, Ressources Humaines, General Counsel
- L'Integrity Hotline (téléphone) ou l'Integrity Line (Web) du Credit Suisse (lorsque le signalement anonyme est disponible, si la loi l'autorise)

Contrôles internes en matière de fraude

- **Séparation des tâches**
Une deuxième personne doit approuver/autoriser toute

transaction ou tout processus afin d'éviter la concentration des contrôles, le contournement manuel des contrôles ou la collusion entre collaborateurs de la Banque.

- **Vérification par téléphone**
Elle est utilisée pour authentifier une demande relative à des données clients (c.-à-d. des relevés) ou de transfert d'actifs (c.-à-d. virements, crédit, titres) en appelant le numéro de téléphone enregistré du client afin de vérifier l'identité de l'auteur de la demande et la légitimité de la demande.
- **Block Leave**
Afin de limiter le risque potentiel de fraude interne, les collaborateurs qui exercent une fonction considérée comme sensible sont tenus de prendre une période de congé de dix jours ouvrables consécutifs au cours d'une année civile. Pendant cette période, les collaborateurs ne doivent pas réaliser de tâches liées à leur fonction, accéder aux locaux de la Banque pour des raisons professionnelles ou utiliser les systèmes de la Banque.

Risques de fraude externe

La Banque et ses collaborateurs sont vulnérables face aux risques de fraude externe, tels que :

- Fraude de la part de fournisseurs
- Fraude relative aux déclarations financières
- Fraude aux moyens de paiement
- Fraude en matière de placements financiers

- Cybercriminalité
- Usurpation d'identité
- Utilisation abusive de la marque Credit Suisse

Normes minimales mondiales contre les fraudes (Anti-Fraud Global Minimum Standards)

Le Credit Suisse a mis en place les Normes minimales mondiales contre les fraudes (Anti-Fraud Global Minimum Standards, AFGMS) en 2021 afin de gérer la fraude interne et externe dans l'ensemble des régions. Afin de garantir le respect des AFGMS, il est important de connaître les normes, par exemple lorsque l'on travaille sur Change Initiatives.

Autres ressources

- [Instruction Escalation \(GP-00012\)](#)
- [Instruction Lutte contre la fraude \(GP-00298\)](#)
- [Instruction Operational Risk Incident Management and Collation \(GP-00260\)](#)
- [Instruction Dispositions US transfrontières s'appliquant aux activités de Private Banking \(P-00025\)](#)
- [Instruction Régimes de divulgation fiscale FATCA et EAR \(GP-00085\)](#)
- [Instruction Risque de conduite \(GP-01058\)](#)
- [Instruction Block Leave \(GP-00387\)](#)
- [Identity Theft 'Red Flags' and associated detection, identification, escalation and reporting requirements supplement to Anti-Fraud \(GP-00298-S03\)](#)
- [Credit Suisse Integrity Lines \(phone and web\)](#)
- [Normes minimales mondiales contre les fraudes \(Anti-Fraud Global Minimum Standards\)](#)