

# Eskalation und Identifizierung von potenziellem Betrug



## Dokumentdetails

Erstellungsdatum	Juli 2022
Herausgeber	Regulatory Anti-Fraud Compliance
Schulungsverantwortliche	Salvatore Bono, Antonios Poutnidis
Ansprechpartner	<u>GG CH Anti-Fraud</u>
Zielgruppe	Global, bankweit

## Zusammenfassung und Kernaussagen

- **Eskalieren** Sie potenziellen Betrug oder verdächtige Aktivitäten sofort.
- Dies umfasst besondere Ereignisse oder Bedenken, die erhebliche Risiken bergen / bergen können. Sie könnten einen finanziellen Verlust für die Credit Suisse / unsere Kundinnen und Kunden nach sich ziehen oder andere wesentliche Reputations- oder nicht finanzielle Schäden für unsere Kundinnen und Kunden, unser Personal, die Credit Suisse und die Integrität der Märkte verursachen.

## Eskalationskanäle

- Ihre Hauptansprechpartnerin bzw. Ihr Hauptansprechpartner ist Ihre Linienvorgesetzte bzw. Ihr Linienvorgesetzter (es sei denn, dies wäre unzweckmässig, zum Beispiel könnte die/der Linienvorgesetzte in das Ereignis verwickelt sein oder das Ereignis nicht angemessen gehandhabt haben) oder andere geeignete übergeordnete Stellen oder das Senior Management.
- Compliance, Human Resources, General Counsel
- Die Credit Suisse Integrity Hotline (telefonisch) oder die Integrity Line (online) (wo eine anonyme Meldung möglich und gesetzlich zulässig ist)

## Interne Betrugskontrollen

- **Aufgabentrennung**  
Eine zweite Person sollte Transaktionen sowie Prozesse bewilligen, um eine übermässige oder alleinige Beherrschung von Kontrollmechanismen, ein manuelles Übersteuern oder Absprachen zwischen Bankmitarbeitenden zu verhindern.

## Rückruf-Verifizierung

Wird zur Authentifizierung einer Anfrage nach Kundendaten (d. h. Abrechnungen) oder Vermögensübertragung (d. h. Überweisungen, Kredit, Wertschriften) verwendet, indem die bei der Bank offiziell registrierte Telefonnummer angerufen wird, um die Identität der anfragenden Person und die Rechtmässigkeit der Anfrage zu überprüfen.

## Urlaub am Stück (Block Leave)

Mitarbeitende mit kritischen Aufgaben bzw. mit Kontakt zu sensiblen Informationen, müssen zur Minderung des potenziellen Risikos des internen Betrugs pro Kalenderjahr zehn aufeinanderfolgende Tage Urlaub am Stück nehmen. Dabei dürfen Mitarbeitende keine Aufgaben im Zusammenhang mit ihrer Position durchführen, keine Bankgebäude für geschäftliche Zwecke betreten und keine Banksysteme benutzen.

## Externe Betrugsrisiken

Die Bank und ihre Mitarbeitenden sind anfällig für externe Betrugsrisiken, wie z. B.:

- Betrug durch Dienstleister und Lieferanten
- Abschlussbetrug
- Zahlungsbetrug
- Anlagebetrug
- Cyber-Betrug
- Identitätsdiebstahl
- Missbrauch der Marke Credit Suisse

## Globale Mindeststandards zur Betrugsbekämpfung

Die Credit Suisse hat 2021 die globalen Mindeststandards zur Betrugsbekämpfung (Anti-Fraud Global Minimum Standards, AFGMS) eingeführt, um internen und externen Betrug in allen Regionen zu bekämpfen. Zur Sicherstellung der Einhaltung der AFGMS ist es wichtig, mit den Standards vertraut zu sein, z. B. während der Arbeit an Änderungsinitiativen.

## Weitere Informationen

- Weisung Escalation (GP-00012)
- Weisung Betrugsbekämpfung (GP-00298)
- Weisung zur Erfassung von Ereignissen (GP-00260)
- Weisung zu grenzüberschreitenden US-Geschäftsaktivitäten (P-00025)
- FATCA-Weisung (GP-00085)
- Weisung Verhaltensrisiko (GP-01058)
- Weisung Block Leave (GP-00387)
- Identity Theft Red Flags Supplement (GP-00298-S03)
- Credit Suisse Integrity Lines (telefonisch und online)
- Anti-Fraud Global Minimum Standards (globale Mindeststandards zur Betrugsbekämpfung)