

# Monitoraggio delle transazioni

**Se un istituto finanziario dispone di un sistema di monitoraggio delle transazioni, tutti i pagamenti trasmessi dal cliente sono sottoposti a una serie di routine di verifica prima che vengano eseguiti. I trasferimenti inusuali, come quelli verso l'estero, vengono analizzati in modo specifico.**

## Verifica automatica di tutte le transazioni

Per impedire l'esecuzione di trasferimenti fraudolenti, alcuni istituti finanziari non solo proteggono l'accesso ai portali di e-banking, ma monitorano anche tutte le transazioni registrate dai clienti. Solitamente la verifica avviene in modo del tutto automatico e in background. Nella maggior parte dei casi i clienti non si accorgono di nulla. Sistemi intelligenti passano al vaglio le diverse caratteristiche della transazione, come il conto del destinatario (versamento nazionale o estero) o l'importo da trasferire, e confrontano queste informazioni con i trasferimenti effettuati dal cliente in passato. Le regole precise seguite per i controlli variano da istituto a istituto e non sono di pubblico dominio.

Questi controlli di plausibilità e confronti con modelli di truffa noti permettono di riconoscere e separare le transazioni anomale prima che vengano eseguite. Quindi il trasferimento viene eseguito quando non sono state riscontrate anomalie. Se è stata rilevata una transazione inconsueta, viene bloccata e sottoposta a ulteriori controlli. In seguito la transazione viene approvata oppure si contatta direttamente il cliente per ulteriori accertamenti.

## Conferma della transazione da parte del cliente

Diversi istituti finanziari richiedono anche, o in alternativa, una conferma della transazione da parte del cliente. In questi casi le transazioni potenzialmente rischiose devono essere confermate dal cliente in modo specifico, in genere per mezzo di un'ulteriore approvazione con lo strumento di autenticazione già usato per il login – p. es. per un singolo trasferimento un ulteriore codice TAN (via SMS se si usa la [procedura mTAN](https://www.ebas.ch/it/mobile-tan-mtan-sms-tan/) (<https://www.ebas.ch/it/mobile-tan-mtan-sms-tan/>) o un ulteriore mosaico da fotografare se si usa la [procedura Photo-TAN](https://www.ebas.ch/it/procedura-photo-tan-procedura-con-tan-ottico/) (<https://www.ebas.ch/it/procedura-photo-tan-procedura-con-tan-ottico/>)).

Non è necessario confermare tutti i trasferimenti. Molti sistemi dispongono di cosiddette black list e white list. Le white list contengono i destinatari di pagamenti affidabili, che possono ricevere pagamenti senza limiti (p. es. assicurazioni, casse malati, uffici delle contribuzioni ecc.). Le black list contengono i destinatari di pagamenti non affidabili, che non possono ricevere pagamenti. Numerosi sistemi registrano, inoltre, i destinatari di pagamenti confermati dal cliente, così da chiedere una sola volta la conferma per trasferimenti che p. es. vengono effettuati ogni mese agli stessi destinatari. Questi destinatari vengono aggiunti alla white list personale del cliente. Per questo motivo, quando il cliente conferma una transazione dovrebbe farlo con grande attenzione.

*Gli istituti finanziari offrono una protezione completa per i dati e le finanze dei loro clienti avvalendosi sempre di sistemi di sicurezza aggiornati.*

[Trasferimento sicuro dei dati](https://www.ebas.ch/it/trasferimento-sicuro-dei-dati/) (<https://www.ebas.ch/it/trasferimento-sicuro-dei-dati/>)

[Accesso protetto ai dati](https://www.ebas.ch/it/accesso-protetto-ai-dati/) (<https://www.ebas.ch/it/accesso-protetto-ai-dati/>)

## **Monitoraggio delle transazioni**

[Custodia sicura dei dati \(https://www.ebas.ch/it/custodia-sicura-dei-dati/\)](https://www.ebas.ch/it/custodia-sicura-dei-dati/)