Transaction monitoring

For as long as a financial institutions implements transaction monitoring, payments transferred by customers pass through special test routine rules before they are executed. Unusual payments, such as international remittances, are therefore scrutinised particularly closely before they are executed.

Automatic checks of all transactions

To prevent fraudulent remittances, individual financial institutions don't just protect log-ins for e-banking, but also monitor all customer transactions they have recorded. These are usually fully automated checks which are run in the background. Customers don't normally notice these processes. Intelligent systems check various characteristics of a transaction, for instance the payee account (for both domestic and international transfers) or the sum of the amount remitted, and compare this information with remittances undertaken by the same customers in the past. The exact checking rules vary from one financial institution to the next and are not publicly available.

These plausibility checks and comparisons with known fraud patterns allow for conspicuous transactions to be recognised and screened out before they are executed. A remittance is only processed if no anomalies are found. In case a conspicuous transaction is found, it is stopped and subjected to further checks. The transaction is subsequently either authorised, or customers are contacted directly for further clarification.

Transaction confirmation by customers

In addition to or instead of this method, various financial institutions also employ transaction confirmations by customers. In this case, customers must confirm potentially risky transactions separately, usually by way of an additional authorisation via the authentication medium originally used to log in - e.g. an additional TAN via SMS with the mTAN procedure (https://www.ebas.ch/en/mobile-tan-mtan-sms-tan/) , or an additional mosaic to be photographed with the photo TAN procedure (https://www.ebas.ch/en/photo-tan-optical-tan-process/) , for an individual remittance.

However, such a confirmation will not be required with all remittances. Many systems maintain so-called black and white lists. A white list contains trustworthy payees which are allowed to receive payments unrestrictedly (e.g. insurance companies, health insurance organisations, tax offices, etc.). A black list contains payees which are not trustworthy and cannot receive any payments. Many systems also remember payees confirmed by customers, so that payment recurring monthly to the same recipient for instance will only have to be confirmed once. These recipients are added to customers' personal white lists. If customers therefore confirm their transactions, they should do so very carefully.

Financial institutions use the most up-to-date security systems to comprehensively protect their customers' data and finances at any time.

Secure data transfer (https://www.ebas.ch/en/secure-data-transfer/)

Protected data access (https://www.ebas.ch/en/protected-data-access/)

Transaction monitoring

Secure data storage (https://www.ebas.ch/en/secure-data-storage/)