"PAYMENTS RE-DIRECTION FRAUD" IN A NUTSHELL

Raiffeisen Bank International
Member of RBI Group

What is it about?

This phenomenon is also known as "Mandate Fraud", "Creditor Fraud" or "Supplier Account Takeover Fraud". It subsumes the change of account details of supplier or customer accounts in combination with debit notes or standing orders, manipulation of credit card activities, or changing employee's salary account details, particularly when a bonus is due.

Warning signals

- any **unexpected requests** to change or update payment details of a regular supplier
- irrespective of telephone, e-mail, letter, or fax, if your company is contacted 'out of the blue' to **amend payment details** always treat this as a **potential warning signal**.
- if the person on the phone is **aggressive** and puts **heavy (time) pressure** on you

Contact

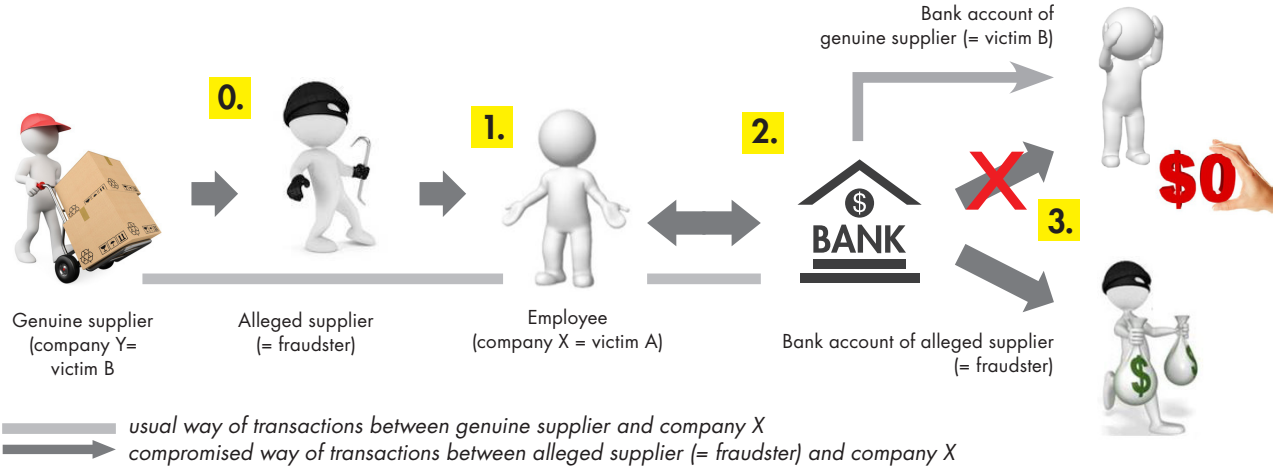
For **questions/suspicions** please contact your Relationship Manager or
RBI Group Financial Crime Management
via **fraud@rbinternational.com**

We are pleased to check and validate your suspicion quickly.

Attention: *Changing bank accounts is an* ***unusual*** *process and therefore any request to update records should be treated with suspicion. Changes should be authorised only at senior level.*

How does it work?

0. Regular payments from Company X to its business partner (e.g. supplier) Company Y.
1. The fraudster contacts the target company X via phone/e-mail/letter, claiming to be a representative of Company Y (e-mails are often sent from the hacked account of the genuine supplier!). The fraudster informs Company X about a change in the account number of Company Y.
2. Employee of Company X updates the account number in the supplier database.
3. From this point every single payment sent by Company X and meant to pay the genuine supplier ends up on the fraudster's account.



Tips to protect yourself

- Treat **any notification to change** details of a supplier's bank account as a **high risk activity.**
- Always verify a request BEFORE implementing the change or completing the payment. Be mindful not to use the contact details provided on the instruction, use established contact details to validate the change instead. (For example, if the update was received by e-mail, verify it via phone or fax, using a previously known number.)
- **Reconcile accounts** on a daily basis in order to identify potential fraud payments quickly.
- **Never** leave invoices **unattended** in the office or on your desk.
- Whenever possible establish at least two specific points of contact with suppliers to whom regular payments are made so that all invoice issues can be raised and confirmed with them.