Payments Re-direction fraud

What is it about?

This phenomenon is also known as “Mandate 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/signals contact your Relationship manager/ servicing branch or the Call center of Raiffeisenbank (Bulgaria) EAD
e-mail: call.center@raiffeisen.bg
phone: 0700 10 000 (Vivacom); 17 21 (Mtel и Telenor)

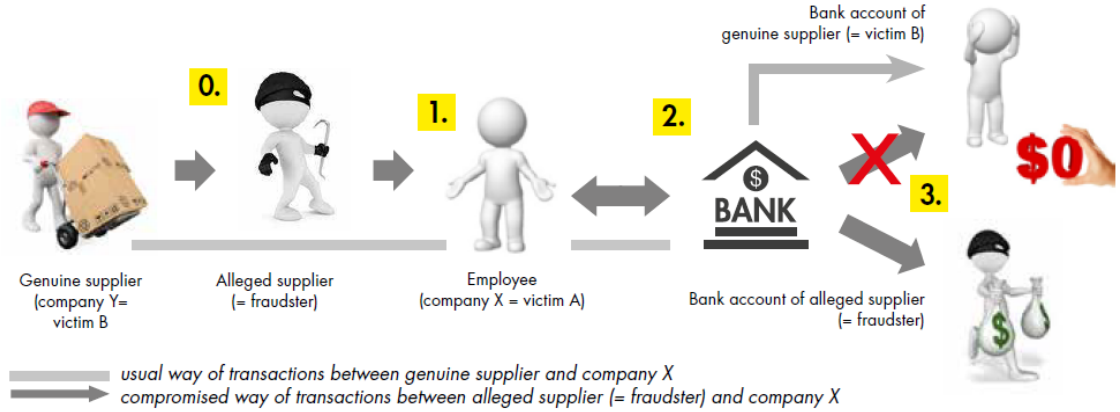
Attention: Changing bank accounts is an unusual process and therefore any request to update records should be treated with suspicion. Changes should be authorised only at senior level.

Fraudulent scheme

The correspondence between two business partners is intercepted and bogus e-mails with genuine invoice details are sent to the payer that purports to be from an existing creditor. The email is meant to notify the receiver of the new (changed) bank account details to which all future payments should be sent. In most cases the payer realizes that he has been defrauded after he has sent at least one payment in favour of the fraudulent account and the original receiver of the funds claims non-receipt of funds.

Key elements – 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.
4. In most cases the payer realizes that he has been defrauded after the business partner informed him that he does not receive a due payment.



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.
- Instruct staff with responsibility for paying invoices to be cognizant of checking invoices for irregularities and checking out their concerns with the company requiring payment.
- Consider setting up a system whereby when an invoice is paid you also send an email to the recipient informing them that payment has been made and to which bank account.