What to do in the event of fraud?

If you suspect fraud in progress, always notify your ING contact or ING Wholesale Banking Fraud operations immediately. Although a transaction made is permanent, we can try to retrieve or block the funds before they disappear permanently from the beneficiary account. Speed is of the essence because the chances of reversing your transaction diminishes with every minute.

Contact

If your ING contact is not available, contact the ING emergency line (+31) 20 228 8800 (24/7).

What to do in case of doubt?

Better safe than sorry: Every suspicious transaction, unexpected behaviour while using e-banking or questionable communication should be reported to ING

What if ING detects suspicious behaviour?

When ING detects suspicious behaviour, for example, questionable login attempts or strange transactions, you could be contacted by ING to verify the validity of the detected event. This contact will, as much as possible, be handled by an ING employee known to you. In case you have doubts about the identity of an ING employee calling, you should always report this either to your regular ING contact or to ING Wholesale Banking Fraud operations

You need to...

If you are a victim of fraud, you need to report this fraud to the designated local authorities (Law Enforcement). ING cannot take legal action on your behalf but can advise you on the steps to be taken. To be able to help you better we require a reference number of the police report within 2 working days of contacting us. Additionally, we require the formal police report once it becomes available. We will ask you to email it to fraude@ing.com.

We require this report in order for the corresponding/beneficiary banks to have an indemnity for any possible actions they are allowed to take.

In case of fraud such as invoice fraud, business email compromise or CxO fraud we also recommend you to verify other transactions made and check for abnormalities in bank accounts (changes), references etc. We often see that fraudsters target a company in more than one way if they have been successful in one attempt.

Our role

In case of fraud we will act as an intermediary between you and the beneficiary bank. We communicate to the receiving bank via SWIFT message that a transaction was effected as a result of fraud and request that the funds will be blocked or returned to the sender.

We try to make direct contact with the beneficiary bank in order to maximize the chance of retrieval. This will give the bank used by the fraudster the chance to conduct an investigation, and decide what is possible for them to do within the applicable laws and regulations. (Note: Funds on a beneficiary account require permission from the beneficiary account holder to refund to the sender account.)

We also perform additional checks to see if any other suspicious transactions have been made. Please do take into account that if transactions fall within normal patterns it could look like a normal transaction for us.

Safeguard your business against fraud

Learn about the most frequent fraud cases which could impact business and learn about the recommendations to protect yourself against it.

Fraudsters are clever, well organised and masters in 'social engineering'. They use deception to manipulate individuals into executing actions or divulging confidential or personal information used for fraudulent activity.

The fraud cases we present on our website are not trivial, they occur daily, worldwide and generate millions in losses.