Covid-19: a global threat requires a shared response

Businesses face a higher fraud risk amid the Covid-19 pandemic. ING is closely monitoring fraud developments in the global financial market to keep our staff, clients, suppliers, and business safe. We kindly ask you to report any fraudulent activity or red flags to us so we can collectively fight fraud.

So, what do we need to be aware of during this unprecedented situation? We have put together a document based on the questions from our clients, other stakeholders, and main regulator – the European Central Bank.

Criminals

Criminals are exploiting the current situation to commit fraud. There is an increase in cybercriminal activities, such as fake emails and SMS phishing attacks. Medical institutions for example, are one of the main targets of malware attacks by hackers.

However, the threat could also come from unexpected sources. Your clients and suppliers may experience significant adverse effects on their business. Others are running the risk of going out of business altogether. As organisations adapt to work in 'crisis mode', internal controls could be circumvented.

Red flags

Any unusual changes in your client's or supplier's behaviour may be a red flag. Here are a number of indicators which may highlight a problem:

- client/supplier not reachable (neither by phone nor email)
- extraordinary/unusual/urgent requests
- confidential requests coming from higher authorities than you are usually dealing with
- presentation of any manual payment requests that do not conform to your procedures, e.g. email payment orders/payment orders without signatures/with non-corresponding signatures/from unusual senders/email addresses/coming from senders who usually do not send such requests
- 'creative' transaction proposals from a customer of supplier (for instance if a supplier would like your company to receive X amount on your company's bank account number and book it to another bank account number while offering a commission for this transaction).
- delays in payments and requests for extensions.

It is of the utmost importance to stay alert and keep a strong line of defence. Here are a few measures that can help keep the fraudsters at bay:

- stick to four-eyes principles
- segregation of duties
- reconciliation of financial administration
- offer awareness training to employees

Fraudsters are using the crisis caused by the Covid-19 pandemic to increase and diversify their criminal and scam activities, as well as exploit fear and uncertainty. These are some of the patterns we noticed:

All channels could be used

Fraudsters use various channels to contact their victims: emails, text messages, Facebook messenger, WhatsApp, etc. They could even use fake phone calls to ask for money. Pay careful attention to the sender of the message.

If you have any doubts but you know the sender, give them a call to verify if they sent the message. Otherwise, do not follow up, do not click on anything and delete the message.

Selling medical supplies online

Several cases of fraud concerning the online sale of medical supplies have been reported to the authorities. Such cases include the sale of fake treatments for the Covid-19/COVID-19 and protective masks, for example. Be mindful about buying medical supplies online.

Always verify the legitimacy of a web shop you have never used before (forums are a good place to look for reviews and remarks from other users). If you have any doubts, use a well-known online supplier or the website of your usual drugstore or pharmacy instead.

Fake messages from the authorities

Fake messages sent by 'official' authorities are meant to steal personal information, passwords and bank credentials. Always check the sender's email address and website before sharing any information or entering your credentials. Remember that your passwords and bank credentials are secret, even for your bank.

Bank e-mails and SMS phishing

Fraudsters may try to impersonate your bank in order to steal money. There are a number of ways to protect yourself from financial phishing:

- never share your bank credentials (even the codes from your card reader) over the phone
- never enter your credentials on a website you've been sent to via an email or text message link. Go to your bank website instead
- learn how to spot a phishing e-mail (see 'examples of red flags' above')

- don't click on links if they are shown in text messages from ING. We do not send messages with links.

Call your bank immediately if you have been a victim of fraud.

Recommendations

- Follow the news and only read information from reliable sources like your local government and authorities
- Visit your bank website regularly for updates on fraud risks

Read the recommendations of Interpol on financial fraud linked to the Covid-19 crisis.

Additional fraud risks from working from home

Many employees are working from home amid the Covid-19 pandemic. Cybersecurity at home may not be as robust as working from the office. A different work environment may also lead to lapses in vigilance. We advise you to be vigilant during this time and so we have provided the following tips as guidance on how to remain cyber secure:

- Use a company laptop or a trusted personal device. Use a company laptop with VPN or VDI, or a trusted personal device with VDI.
- Use a trusted Wi-Fi access point. Use your home Wi-Fi, or your work mobile (4G) as a hotspot and connect your laptop to your mobile. Do not use public and hotel Wi-Fi for work.
- Ensure all devices are kept up to date and install the latest anti-virus programmes on personal computers.
- Use authorised communication methods only and keep data on your company systems. Only use methods approved by your own company for communication with clients (e.g. email, telephone) and when sharing files. Do not email or transfer any company documents to personal email accounts or devices. If you need help while working from home, please contact your own IT Service- or Helpdesk. Use your company tool for conferencing, don't use other tools for data protection and licensing reasons.
- Watch out for phishing emails and Business Email Compromise. Phishing emails create a sense of urgency to coerce you into divulging confidential information (such as usernames and passwords or customer information) or into opening malicious attachments by disguising as a trustworthy entity. Business Email Compromise or CxO fraud is a type of scam where cybercriminals pose as a senior executive by emailing an employee with the instruction to urgently initiate a transaction or payment. Always verify the sender's address when receiving (unexpected) emails, especially those containing requests for urgent action. Hover over any hyperlinks to verify the legitimacy of websites. Check the sender of the email by clicking on the display name. Be wary of unexpected emails that ask you to click on a link or open an attachment.

  Read more about corporate fraud

- Be vigilant for vishing (voice phishing) attacks. Fraudsters will conduct malicious calls posing as team members or colleagues from other teams and locations. Be suspicious of all unknown callers, especially if you are asked for company-related data, personal or financial information. Ask for identification. If the caller ID is shown, record it.
- Be aware of who might be listening to your conversations. If working in public areas cannot be avoided, ensure that others cannot easily watch over your shoulders. Do not handle confidential data in public areas, whether in digital or physical formats. If you possess a privacy filter, install it on your laptop. Be mindful of your environment when discussing confidential matters in conference calls. Also take into account smart devices like Alexa.
- Always lock your workstation when stepping away from it. Even when at home, others can intentionally or accidentally misuse your computer even if you are away for a few minutes. Emails could be sent from your account, files could be changed or deleted, and confidential data could be accessed.

Regular security and fraud

ING regards knowledge of fraud and sharing this information with clients as the first line of defence against fraud. By learning about the types of scams and countermeasures used to prevent these, your organisation will be better prepared to identify fraud and reduce it significantly.

Read more about corporate fraud

ING continuously invests in upgrading software and improving security measures to prevent any misuse of our online banking services. However, secure online banking is a shared responsibility between us and you, our clients. Please make sure you properly secure your computer and (network) environment against misuse by unauthorised entities.

Read more about online security

What to do in case of fraud or suspected fraud

If the fraud is in progress, meaning the payment has been sent for example, take the following measures:

- Immediately report this to your regular ING contact. Provide your contact with the following details:
  - initiating account number
  - beneficiary account number
  - amount
  - date of transaction
  - channel used to initiate the payment
  - reference number of the police report (can be handed in on a later date).

- If your ING contact is not available, please call ING Wholesale Banking, Fraud operations at +31 20 584 7840. By calling your bank quickly, you will increase the likelihood of recovering the embezzled funds. Even though a transaction has been made, 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 diminish by the minute.

  ING Wholesale Banking Fraud operations availability:
  Monday to Friday: 7:00 am to 0:00 am CET
  Saturday: 8:00 am to 5:00 pm CET
  Sundays: closed

- Contact fraudpayments@ing.com outside working hours.

Fraud detection well after the fact

After 24 hours it is practically impossible to recuperate stolen amounts. If the fraud occurred a while ago, it is not likely that the embezzled funds can be blocked and retrieved. In this case, please report the case via e-mail to fraudpayments@ing.com.

What you have to do

Reporting to Law Enforcement. A copy of the police report is necessary for us and for the beneficiary bank acting as an indemnification. Please find the contact information for your local police department. Your local police department has a non-emergency number you can call to file a report. Request a copy of the police report for your records. Not only will you need a copy for your records, you also need to submit a copy of the report, or the reference number for the report, to us or other entities as you work to resolve the situation. ING cannot take legal action on your behalf, but can advise you on the steps to be taken.

If you want to learn more about the general measures ING is taking to keep staff healthy and safe, as well as how we ensure that our services to customers are not compromised please download ING's response to the Covid-19 pandemic.

Disclaimer

This information is provided to you solely for informational purposes in order to make you aware of the most frequent cases of fraud and provide you with recommendations to protect yourself against it. This information does not ensure that your company, acting upon these recommendations is or will be protected against any occurrence of fraud detailed in this information. No rights can be derived from the use of and reliance on the safeguards you take by following up these recommendations. ING does not accept any responsibility or liability with respect to your reliance on and the actions you take as a result of these recommendations. This disclaimer is governed by Dutch law.