How to prevent fraud going forward?

Simple measures can help to prevent fraud dramatically. Use the following tips to mitigate risk of being a victim of fraud:

Do's and don'ts

Do:
- Educate your employees
- Use antivirus and up-to-date software
- Only install software from trusted sources
- Be suspicious of any phone calls and emails from individuals you don't know
- Always check email sender to ensure his email address is legit

Don't:
- Use outdated software
- Share your logon credentials
- Click on links received unexpectedly
- Share PC screen with persons that you don't know

Risk and controls

- Create detailed records of customers/suppliers/payees
- Validate all new/change beneficiary account requests with a phone call to a trusted contact
- Confirm unexpected requests for transfers by a phone call
- Implement robust procedure for changing beneficiary account/information
- Implement '4 eyes' check procedures and validate internally by calling relevant parties

Need help?

If you have any questions or concerns, please reach out to your local Relationship Manager

2020.03 Danske Bank A/S CVR-nr. 61 12 62 28 - København

Fraud prevention Do's and Don'ts

Global Fraud Management
Version 1.1

Danske Bank

How do you spot fraud?

Businesses becoming victims of fraud is a growing issue today. It can be difficult to spot, as fraudsters aim to exploit human psychology and other social engineering techniques to commit their crime. Awareness is key in fighting fraud and the below advice can help you to protect your business from the risk of fraud:

Have you noticed?

- Calls with over-complimentary or aggressive language
- Changes of usual tone, requests insisting on rushing a payment through
- Changes in an email address or it‘s appearance
- Changes in contact names or details provided
- Poorly written requests

Is someone asking you to...

- Change contact details or add new ones
- Receive or act on unusual instructions
- Click on unexpected links
- Not follow usual procedures
- Deal with an unknown payment beneficiary
- Provide payment confirmation via email
- Make a transfer to a new or changed account
- Urgently proceed with a transfer
- Transfer a large part of an account balance
- Transfer a large amount of funds just before a holiday season

Most common fraud types

- CEO fraud – criminals will impersonate the executive manager and ask an employee to make an urgent transfer
- The employee may be from finance or have the ability to instruct finance or other relevant to execute the payment.
- Beneficiary account change – Fraudsters will gain access to a business partner’s email and request to change beneficiary account details;

Need help?

If you have any questions or concerns, please reach out to your local Relationship Manager

What to do if you and your business have become victim of fraud?

If you notify us about a fraud attempt on your business, we take all necessary actions to initiate recovery of the funds lost due to the criminal activity. Please find information below on what we will need from you and a timeline showing when you will be updated on the case:

Bank actions

- Request for cancellation SWIFT messages are sent to all involved financial institutions
- Involved financial institutions contacted via email and phone to ensure they are working on the case
- Investigation of fraudulent activity on your accounts, ensuring every suspicious payment has been cancelled

Company actions

- Provide us with a first point of contact
- File a police report in both the remittance and ultimate beneficiary jurisdictions. Obtain a copy of the report or save a crime reference number and provide it to us
- Provide full transaction details and as complete as possible background details on the fraud incident
- Be prepared to provide an indemnity to facilitate bank-to-bank recovery
- Independently review all recent transactions and logs for other suspicious payments/unusual activity across all bank accounts
- Initiate an internal investigation. Ensure that any potential evidence is retained and secured. Examples of evidence include email correspondence, audio logs, desktop PCs, etc.
- Alert suppliers/vendors about possible fraudulent invoice/account payee change requests

Follow-up

- We will get in contact with you within the first 24 hours after you inform us about the event. We will update you as follows
  - 48 hours after you inform us
  - Five days after you inform us
  - When we are about to close the case

Need help?

If you have any questions or concerns, please reach out to your local Relationship Manager