TRANSFER FRAUD

HOW CAN YOU PROTECT YOURSELF?

BNP PARIBAS

The bank for a changing world

Fraud and cybercrime: the latest developments

IMPERSONATION FRAUD IS EVOLVING

Transfer scams are wreaking havoc all over the world. Certain large companies are being targeted by up to three or four fraud attempts each day.
Recently in Hong Kong, fraudsters made a US company suffer losses of 47 million dollars! In particular, fraud perpetrated by a fake supplier who requests that an IBAN be amended remains as a dangerous ruse for companies that are yet to tighten up their procedures.

Fake CEO scam
A fake director insists that his victim send a confidential and urgent credit transfer.

Fake technician scam
A fake bank technician "helps" his victim process a payment test.

Fake vendor scam
A fake supplier or landlord asks the victim to amend their bank details.

MALWARE FRAUD IS ON THE RISE

Since 2015, companies have also been targeted by large-scale attempts to infect their networks with malicious software that is sent by e-mail. Hundreds of thousands of PCs have currently been contaminated by the DRIDEX program. The program takes control of the PC, launches credit transfers, and then steals the company's supplier and customer lists.

THE RISKS AND HARM CAUSED ARE NOT PURELY FINANCIAL

Aside from financial losses, these acts of fraud can traumatise those who have been affected, and they can lead to job losses or even bankruptcy. They can also do an untold amount of damage to the image of the company that has been targeted.

DATA THEFT POSES A MAJOR RISK

Companies hold valuable information about their customers (contact details, invoices, etc.). Scammers attempt to steal this data by penetrating IT systems, spreading malicious software, or even by e-mail or telephone (e.g. by stealing a customer's identity).
Data theft can have disastrous consequences for a company (especially for large billers such as telco's, utility companies, large property management companies...), such as vast amounts of unpaid invoices, loss of image, commercial risk, etc.

How can you protect your company?

TRAINING AND AWARENESS

Fraudsters always exploit human failure. This is why it is important to train your employees. Sending them e-mails on the subject is not enough; train all of your teams on a regular basis to become more aware of the risks of fraud, cybercrime and data theft. This includes your accounting department, treasury department, purchasing department, switchboard operators, new arrivals and temporary staff, etc. And, do not hesitate to discuss the risks with your customers and suppliers.

SEGREGATION OF DUTIES AND DATABASE PROTECTION

Ensure that there is duty segregation in your accounting and treasury tools. Set limit amounts that are adapted to your company's operations and restrict the amount of funds that are available. Avoid transfer orders and validations that are made on paper.
The databases containing the details of your customers and suppliers must be protected (encryption and restricted access).

COUNTERPARTY AUTHENTICATION

Circulate written procedures for the authentication of counterparties, especially in relation to the following cases:

- A supplier requesting amendments to their bank or telephone contact details,
- Any person asking for an invoice to be reissued or for information about your systems, procedures or bank details (a customer, tax inspector, central bank, market research worker, etc.),
- A technician offering assistance with your cash management tools, electronic payment terminals, and so on.

CONTROLS

Ensure that the list of transfers made is checked every day, paying particular attention to large international transfers. Ask for a paper document before validating any payment. Ensure that there are regular audits and that internal inspections are performed.

ANTI-FRAUD GOVERNANCE

Fraud prevention is a problem to be tackled in various areas, including the treasury department, accounting department, purchasing department, IT management, HR (training) department, internal control, etc. Implement governance designed to combat fraud in order to continuously improve your systems and procedures. You should also work with your partners, e.g. banks, software vendors, insurance providers, etc.

BNP Paribas SA has a share capital of 2.490.325.618 Euro
Registered office: 16 bd des Italiens 75009 Paris
RCS Paris n° 662 042 449 Identifier CE FR 76662042449
Registered as Insurance broker at ORIAS n° 07 022 735
January 2016.

BNP Paribas is here to help

CUSTOMISED DIAGNOSIS

Relationship managers are always available to carry out a free customised fraud prevention assessment that quickly allows you to identify areas of improvement for your company.

TRAINING AND AWARENESS

To help you to raise your staff's awareness, BNP Paribas can offer you:

- Free training kits and brochures,
- Regular events on the subject of fraud,
- Recommended expert trainer contacts.

SEGREGATION OF DUTY AND LIMIT AMOUNTS

Our cash management officers can give you advice on the tools you use and the way your outgoing transfers are organised, as well as on our secure solutions for cheques, card collections, direct debits, and so on.

COUNTERPARTY AUTHENTICATION

BNP Paribas will soon be able to offer you a bank details verification service called "SEPA Mail Diamond", which will be available for French accounts as a first step.

BANKING CONTROLS

Where BNP Paribas detects a suspicious transaction, your relationship manager will call you in order to make sure that it is genuine. We can also propose to set customised checks thanks to our "**Secure Flows**" offer:

1. **Definition of anti-fraud filters** according to domiciliation of your partners:

List of **authorised coutries**

List of **authorised beneficiaries**

+ Optional control trigger threshold.

2. **Optimal reporting mode** in case of credit transfers rejected for anomaly

With Secure Flows you can add the ultimate control of the bank prior to the execution of your transfers

BNP PARIBAS

The bank for a changing world