BNP PARIBAS

The bank for a changing world

FIGHTING AGAINST VENDOR SCAMS: CORPORATE BEST PRACTICES

There is no miracle solution to protect against fake vendor scams (bank details fraud). Account payable departments generally apply rules of common sense and more or less restrictive procedures. In this article, we offer a review of some corporate best practices, so that you can benchmark your company or grab some ideas.

BANK DETAILS CHANGE FRAUD, A VERY POPULAR SCAM

Fake vendor scam is relatively simple: first, a fraudster identifies one of your first-tier suppliers. He contacts this supplier, acting as one of your accounting officers or your external auditor, etc. and asks about information relating to the current payment of invoices. Second, he contacts you, acting as your supplier. He notifies a **bank account change**, and sends you real invoices, with modified account number and bogus telephone numbers.

- This fraud scheme is very dangerous, because it attacks **normal processes** of the company (unlike CEO scam) - what's more natural indeed as a supplier payment?
- This fraud is generally **detected too late** to expect a fund recall; and it can last for several months, because the scammer generally manages to urge the real supplier to wait.
- Some people are unaware that generally, recipient's banks do not check the **beneficiary names** shown in the transfers.

The prejudices at stake depend on your supplier payments, but can reach **very important amounts** (up to a significant portion of your turnover!). Proofs of this are the vendor scams of more than $ 100 million suffered by Google and Facebook in 2017...

FIGHTING AGAINST FRAUD ATTEMPTS: PREVENTION AND ACTION

To control **CEO scam risks**, systematic awareness and segregation of duties in payment tools are generally sufficient.

Conversely, in the event of a fake vendor scam, there is **no miracle solution** but a **set of good practices**: defining **clear and formalised procedures**, using **effective tools**, and building a **culture of risk** in the company - the objective and the challenge being to have solid "KYS" processes (**know your supplier**) to control your risk.

Formalising a few simple rules

The basic rule, implemented by almost all businesses having realised the risk, is to **authenticate any bank account change** (which can be notified by email, by letter, by email, on invoices, by phone, etc.):

- Most companies ask the account payables department (or purchasing department) to **call back the usual contact** with the supplier to authenticate account modification notifications;
- Of course, this call-back is carried out using **safe telephone numbers**, and not those reported on the invoice or the bank account change notification.

Some organisations apply additional best practices, for example:

- Achieving the call-back **on receipt** of the bank details change notification, in order to avoid achieving this check in a hurry, just before making the payment;
- Assigning **team managers** the responsibility for validating any bank account modification, in order to empower the local management and avoid mistakes made by less aware employees (newcomers, etc.);
- Use two different channels (for example, email and phone) if the new bank account is held in a **foreign country** (besides, some large corporations require their "first tier" suppliers to open accounts in domestic banks, to simplify their controls);
- In the same way, make **more stringent checks for larger suppliers** (for which the risk of fraud is inherently higher).

Note: many companies require a **bank certificate for the authentication of the new account**. However, it is extremely easy for a fraudster to **create a false bank certificate**. That is why some companies ask this certificate directly to the beneficiary's bank (with uncertain answer and processing time...).

Sound management of supplier contact details

It is useful or even essential to extend these "know your supplier" procedures by strictly **managing vendor contact details** used in call-back and **email addresses** used to communicate with suppliers:

- Achieving verification in case of **change of contact details** of usual correspondents;
- Allowing only **designated people** to administrate the contact details used to call-back suppliers;
- Teaching employees to **check correspondent's email addresses**, by carefully looking at domain names, which may resemble that of supplier, differing by only one character - for this, it can be useful to look at detailed email headers; see some tips on this **page**.

Note: by using email addresses that look like yours and that of your correspondent, scammers can achieve to interfere in your email exchanges with your vendor. When you send an email to your supplier, fraudsters receive it and forward it to your correspondent; and can transmit your supplier's answer to you as well. In this case, the illusion is perfect!

Effective tools

To implement such procedures, companies must use **tools adapted to their size and organization**:

- It is necessary to have a **secured directory** with your usual correspondent contact information. In some companies, this is implemented in the ERP or other management tool, accessed only by authorised persons;
- However, other structures prefer simply using a **paper notebook** available only for employees of the account payables department! Or some accounting services simply use contact information listed on **previous invoices**, which are a priori safe (without guaranty however);
- It is also necessary to establish **lists of approved beneficiary accounts** in your payment tools or in your ERP. Any creation of new third party account should be detected and subject to validation by entitled employees, following the application of the proper call-back procedure;
- In addition, many BNP Paribas clients use **Secure Flows**, a solution which allows defining anti-fraud filters according to the domiciliation of your partners and country risk, and performing an ultimate control of the bank prior to the execution of your transfers.

To fight this rising threat, the market starts providing additional solutions:

- In France, BNP Paribas offers **IBAN Check**, which allows you to check the **consistency of an IBAN and a SIREN number** (French corporate registration number). This service is available via a secure website or via usual e-banking channels (for example with EBICS, SWIFTNet...) and will be progressively extended to some other countries.
- Some companies prefer subcontracting the management of supplier contact information with a **service provider**, according to precise specifications, allowing them to outsource part of the risk. Some of these service providers can offer insurance covering the risk of credit transfer fraud.

Building a culture of risk

Procedures and tools are not all. Fraudsters are very imaginative and persistent, and they almost always exploit **human failure**. To defeat scammers, it is essential to rely on your employees, which are the first line of defence of your business.

It is crucial to hold **awareness sessions** about vendor scam related risks (with concrete and varied examples), and **train your employees** (including newcomers and temporary employees) about the "know your supplier" procedures you have put in place. Do not hesitate to ask your relationship manager our **training kit** "Credit transfer fraud", which could be of help.

To defeat scammers and protect your own clients, which could also be targeted, it is also important to **avoid communicating information to scammers**. You should therefore educate your employees about the risk of information dissemination, and teach them:

- To **avoid spreading information** on the Internet (social networks, blogs, websites ...);
- To **check the identity of any person requesting information** (head-hunters, survey institutes, unknown colleagues, tax inspectors, etc.);
- And above all, to **check all request regarding your invoices**, your company's premises and rents, payments, collections, clients, suppliers, bank account numbers, etc. (pay attention to fake customers, fake auditors, fake tax administration...), **using safe contact details** or calling the switchboard.

For this purpose, feel free to request our **training kit** "Protecting information."

Finally, BNP Paribas offers **risk assessment sessions**, to help clients identify some areas needing improvement and fight fraud together.

Please contact your relationship manager, who is available to advise and help you, and feel free to share with him tips that your company may be using to protect against vendor scams, which is not mentioned in this article, and that could be of interest to others.