Preventing wire transfer fraud

SIACI SAINT HONORE

1. Impersonation of company executives

Since 2012, a large number of groups have been targeted by criminals specialising in wire transfer fraud, dubbed the "fake chairman scam" by French police. The finance departments of foreign subsidiaries receive a phone call, allegedly from the group chairman, requesting an urgent and confidential transfer of funds to an account in Hong Kong, Switzerland, Cyprus, or even Warsaw, for the purpose of financing an acquisition.

Given the magnitude of the phenomenon, the General Directorate for Internal Security (DGSI) has approached leading French groups to raise awareness of this new threat. This phenomenon which previously only involved large companies can now affect businesses of any size. The misappropriation of substantial amounts may even jeopardize the future operations of companies which are targeted in this way.

Cumulative losses suffered by French companies in 2014 were in the region of €300 million while more than 700 scams were recorded by the French investigative services.

Evidence shows that companies which succeeded in avoiding or limiting such losses had specific procedures in place for the management of international transfers. The employees who were contacted by the fraudsters were familiar with these procedures and applied them successfully. These simple protective measures include a dual signature procedure which must be authenticated by the bank for the transfer of large amounts.

2. Misappropriation of payments to suppliers and lessors

This is a simple fraud committed by a third party who targets a company's finance or accounts department. It involves a fraudulent request to change the bank details of an actual supplier already listed and registered with your company or your lessor.

1. You receive a telephone call from a person claiming to be your supplier or lessor informing you that their billing and payment services are being relocated abroad and that their bank details will therefore need to be updated.
2. These requests are then followed up by a fake email (using IP spoofing or a fake email address similar to that of your usual contact) or a fake letter (on company stationery and including the correct ID references of the supplier or lessor) confirming the change.
3. The letter is sent to the accounts department which checks the supplier's apparently valid reference number and notifies your bank of the new account details.

4. Once the information has been sent or entered into your SAP system, the transfer orders provided to your bank to settle the fake invoices appear to be genuine.

5. On receipt of the next invoice from your supplier, or on the next scheduled payment date, the funds are transferred to the fake account.

These scams are uncovered when your supplier or lessor chases payment of their invoice which of course they never received. In the meantime, the recipient account has been emptied and closed by the fraudsters.

3. Impersonation of bank employees

As in the case of the "fake chairman scam" you may fall victim to manipulation by fraudsters posing as an employee of your bank. They use information previously gathered on your staff and company structure (organization chart, job titles, authorized persons, vacation schedules, specimen signatures etc.). These fraudsters are very well informed, persuasive, and sometimes have associates working inside the company.

1. An employee of your company receives a telephone call informing them of a technical procedure to be carried out on the bank's servers or a problem involving remote transmission or security.

2. This call is often followed up by an email bearing the bank's logo.

3. The individual poses as an IT engineer from the bank. They're very knowledgeable about your organization and the banking procedures in place for telematic transfers.

4. This individual uses the pretext of testing tools for the exchange of banking files "for the introduction of the SEPA[1] system" in order to obtain the login codes and passwords. They will also ask for a copy of the bank transfer confirmation to be sent by fax including the signature of an authorized person.
In some cases they will ask the employee to call a number which plays the same on-hold message as your bank.

5. Having supplied the fake bank account, they then request the company to carry out an international transfer to finalize the remote transmission test.

1. In 2008, European banks introduced the SEPA system for the transfer of funds in euros from one account to another within the SEPA area with the same ease and at the same price as domestic transfers. On August 1, 2014 SEPA transfers and SEPA direct debits permanently replaced national transfers and direct debits for both national and cross-border (intra-European or international) payments.

4. Some tips to help improve your security

a. Be alert to possible scams involving suppliers, particularly within the finance department

- Confirm the identity of the person making the request to change the bank details. Is the request coming from the usual contact and the usual email address?
- Check your previous dealings with this provider: have any other changes to the standard details been requested? Do transactions with this supplier involve large amounts?
- Compare the headed stationery with letters from the same supplier and check the request with trusted contacts at the supplier company.
- Within the accounts department, any changes to contact details (particularly bank account details) for suppliers, clients or other business partners must be independently checked by members of the accounts team and confirmed with the client or supplier. As far as bank account details are concerned, only an original copy of the information will be accepted.
- Be sure to reconcile payments and accounts on a regular and frequent basis.

b. Train and inform your employees

Any members of staff who may be targeted should be alerted as a matter of priority in all countries where your company operates. Employees should be made aware of this type of fraud, not only in the finance department, but also in any departments which may be in contact with third parties. You should circulate this warning to all staff and to head office but also to all of your subsidiaries.

Supporting employees in combatting fraud

- Designate a dedicated point of contact who must be notified in cases of suspected fraud (e.g. the legal or compliance director).
- Send out regular emails and memos with reminders of the tactics likely to be employed by fraudsters, characteristics of suspicious payments, internal transfer procedures and the existence of a dedicated point of contact for reporting suspected fraud. Use a personalized message from a member of the management team confirming they will never directly request an urgent payment to be made in defiance of internal control procedures.
- Issue a recap of the procedure to be followed if a member of staff receives an urgent call from someone using threats, intimidation or blackmail to order a payment and/or posing as company executive. The employee should terminate the call and immediately inform the dedicated point of contact.
- In all cases, a return call should be made to the person who allegedly issued the instruction to

check if it is indeed genuine. Care should be taken, however, to call this person on the number listed in the company's files and internal directories and not on the one shown on the headed stationery which may be fake.

Conduct a stress test

Simulate an attempted fraud either in-house or using a firm specializing in business security. This test helps to generate feedback by raising employee awareness. It also detects weaknesses within each company which can then be addressed.

Empower employees

- Reduce the number of persons authorized to send information to external contractors.
- Be wary of social networks (Facebook, LinkedIn etc.).
- Circulate a charter reminding employees of best practice when using modern means of communication (no information about the company, keeping profiles private etc.).
- Include a heightened requirement for confidentiality in contracts of employment.
- Inform employees that any breach of internal procedural rules represents grounds for dismissal (constituting serious misconduct with no notice or severance pay).

c. Implement effective payment checks

Introduce a dual signature or dual authorization process within the company

The requirement for two signatures is highly recommended for all payments and should be mandatory for payments above a certain amount. Ideally, employees with the power to authorize payments should be divided into 2 groups, for example "A" (authority to act on behalf of the company) and "B" (based on their responsibilities and therefore their ability to confirm a payment).

- A basic-level accountant should not be able to order a transfer.
- Minimize the number of people who can issue instructions for manual payments.
- Separate the duties between the person preparing the transfer and
- Implement a dual signature procedure for amounts over a certain value.

Strengthen banking processes and relationships

The payment authorization procedure described above must be confirmed with your banks. The banks' employees should be asked to report, or even block, any unusual transactions involving the transfer of funds (unusual in respect of the amount or the beneficiaries or payments to an account in an unusual country or an offshore account, because of the reason given, etc.).

- Establish a confirmation call procedure with the bank to verbally confirm transfers over a certain amount (confirmation of the amount and the recipient by the signatory).
- Centralize banking relationships by limiting the number of banks used by the company.
- If any new companies are acquired, their bank accounts should be analysed and transferred.

Enhance the effectiveness of emergency procedures

Urgent transfers should not be exempt from internal controls and specific procedures should be put in place to authorize urgent transfers.

- Appoint a dedicated point of contact to handle emergency procedures.
- Make it mandatory for the staff member to note down the date and time when they obtained approval from the dedicated point of contact for an emergency transfer.

Develop the use of secure payment methods

Secure payment methods should be used wherever possible. For example, electronic signatures (including with biometric authentication) are now offered by most financial itermediaries and may discourage someone who is being persuaded or forced to copy or reproduce a handwritten signature.

Any non-secure payments (fax, paper, phone, e-mail or checks) should be limited and a corresponding entry must always be made beforehand in the company accounts.

d. Monitor the data provided about your company

Before carrying out their attack, the scammers conduct a thorough "social engineering" investigation. This allows them to obtain information on the company, its directors, its organizational structure, personal phone numbers for the managers and employees, their habits, their family lives and schedules, employee absences, how the company operates, documents bearing the signature of company executives, the company stamp etc.

Raise staff awareness on the use of social media

- Educate all members of staff on the risks posed by the new media, which have become a great source of information for fraudsters. The company should issue its employees with security guidelines prohibiting the posting of professional (and especially confidential) information on social networks.
- Ensure employees do not pass on private and confidential information by phone to their contacts (such as contact details and other information on suppliers, payment security measures in place etc.).
- Advise switchboard operators to handle any unusual requests with care. For example, an unidentified caller making a request such as "Put me through to payments" should be treated with caution and be subject to a special procedure.

Ensure information and communication systems are secure

- Ensure intranet access is secure.
- Carefully manage your internal and external communication media (website, blogs, brochures and newsletters).
- Limit disclosure of information on the organization of the company, its management structure and schedules.
- Limit disclosure of personal information (specific telephone numbers and job titles).
- Limit information on internal events (corporate balls etc.).

Keep a check on company information

Companies are required by law to disclose a number of documents which are made available on websites such as *infogreffe*.

- You should only publish documents which are required or **mandatory** by law (current statutes and minutes).
- Take care with filed documents which include the signatures of the chairman or associates.
- Strike a balance between the interests of transparency and the risk of fraud (by not providing overly specific details in the reference document).

e. What to do if you fall victim to a scam

1. Immediately inform the banks

- Immediately notify the issuing bank that the order is fraudulent. Transfers are normally instant and irreversible once the funds have been made available to the beneficiary. In exceptional cases remedial action may be possible after the event.
- Have the funds blocked as soon as they've been traced, if they're still being held in a bank, as once transferred to a customer account, it's very difficult to block them. It's important to involve your bank and the local bank to which the funds were transferred.

2. Contact the police without delay

- Immediately notify the SRPJ (Regional Judicial Police Department) who will in turn notify the Serious Fraud Office (*Office central pour la répression de la grande délinquance financière*).
- Provide details of the circumstances surrounding the fraud (source of the order, information on incoming calls, etc.) which will assist the police in their search for the fraudsters.
- You should also alert the authorities in the country to which the funds have been sent so that any funds still being held by the bank can be blocked.
- Contact your banking advisor straight away if the transfer has gone ahead so that the funds can be traced. Transfers are completed in just a few hours so the time factor is crucial.
- Inform your employees of the attempted fraud. Fraudsters assume that management will tend to keep the attack confidential and will use the information already gathered to attempt further scams. Evidence shows that new attempts will almost always be made, unfortunately resulting in further transfers of funds.

3. Monitoring threats or attacks

- Keep a record of unusual requests and contacts, especially from suppliers. This history of previous suspicious incidents can be referred to when taking calls.

SIACI SAINT HONORE is highly experienced in the issues surrounding fraud, extortion and the misappropriation of funds. Our specialist team assists and supports a large number of companies through risk analysis and the setting up of insurance policies to cover losses resulting from incidents of this kind. We would be pleased to answer any questions you may have and to contribute to your discussions on this sensitive matter.

SIACI SAINT HONORE

18, rue de Courcelles
75008 Paris
Tel: +33 1 44 20 99 99
www.s2hgroup.com

Contact : **Mickaël ROBART**
Financial Lines Departement
mickael.robart@s2hgroup.com
Tel: +33 1 44 20 94 53

SIACI SAINT HONORE - 18, rue de Courcelles - 75384 Paris Cedex 08 - Tel: +33 (0)1 4420 9999
Fax: +33 (0)1 4420 9500 – Insurance brokerage – ORIAS no. 07 000 771
A French Société par actions simplifiée, with a capital of €14,143,816.
Registered in the French "Registre du Commerce et des Sociétés de Paris" under number 572 059 939 RCS APE 6622 Z
Intra-Community VAT identification number: FR 54 572 059 939