Financial Lines

FRAUD ALERT

We have always, and continue to see frauds involving collusion between employees and suppliers, but over recent months we have noticed an increase in "Payment Diversion" and "Fake President" frauds.

Payment diversion Fraud

This is a simple fraud committed by a third party targeting a company's accounts/finance function and entails a fraudulent request to amend an actual supplier's banking details recorded with the company.

KPMG posted this as a News Release alert in December 2012 (www.kpmg.com/uk/en/issuesandinsights/articlespublications/newsreleases/pages/millions-lost-as-fraudsters-expose-a-mandate-for-change.aspx) and Baker & Mackenzie as a client alert in April 2012 (emailcc.com/rv/ff0008f7d5c8a461650f0286ae488f295c43c3d7). Such requests may then be followed up by a fake email or letter confirming the change.

"Fake President" Fraud

Furthermore, we are starting to see external frauds based on a "Fake President" scam. These frauds are generally based on a very simple but audacious scenario. The fraudsters impersonate a group executive (the President, CEO or CFO, for example) and call a manager, an accounts payable clerk or any other employee they think could be of use to their scheme in a subsidiary requesting them to execute an urgent and confidential (and generally off-shore) payment. This may well be followed up with an email (with what might appear initially to be a perfect replica of the genuine email address or an explanation of why a "special" email address is being used).

Once the transfer has been made and the funds received by the fraudsters they are immediately channelled to a further fraudulently opened off-shore account. This topic has also been posted as a client alert by Baker & Mackenzie this April (bakerxchange.com/rv/ff000f66ad4ea1d8a70e8ae14b41a77afc53565c).

To date mainly French companies (generally subsidiaries of European groups) or companies with a strong French "connection" have been targeted by the Fake President scam and tens of millions of Euros have already been embezzled. A French documentary aired on the channel M6 investigated this matter and mentioned a tally of 100M Euros of embezzlement last April.

You will find attached our guidance of suggestions enabling you to prevent and/or to react to these fraud attempts.

We strongly urge you to pass it on to your subsidiaries or branches.

Bring on tomorrow

www.aig.dk

AIG Europe S.A., Osvald Helmuths Vej 4, DK-2000 Frederiksberg, Danmark Tel.: (+45) 9137 5300 Fax.: (+45) 3311 3340

FRAUD ALERT

Guidance Notes

The aim of this guidance note is to heighten vigilance in the face of any attempt by outside third parties to try and contact company staff.

1 Inform Staff

As a matter of priority, alert all those that could be targeted across all geographies of your organisation and raise their awareness to this type of fraud; not just at the Finance function level but also all services likely to be in contact with third parties. This means that the alert must be general in its distribution and it must reach all foreign subsidiaries. Management needs to support the communication – companies are being targeted every day.

2 Ensure robust global corporate processes are in place to mitigate the risk

(a) No important instruction (payment or otherwise) should be given by telephone or by e-mail. Only requests that are received in writing and on letterhead should be acted upon, with a "call back" to the person purporting to send the instruction to check authenticity. (Beware though, that the call back should be to the person's telephone number as taken from internal company records, not that on the letterhead as this could have been fraudulently altered).

(b) Be careful and know who you are speaking to on the phone and keep logs of unusual callers and requests so these can be referred to when taking calls, to see the call history

(c) Escalate to the relevant person any note purportedly from senior management where the tone or style is unusual and/or where unusual grammatical or typographical errors appear.

(d) Ensure employees do not volunteer private / confidential corporate information to callers (such as supplier numbers and details)

3 Be alert to potential supplier scenarios, particularly those within the finance function

(a) Confirm who is making the request to change bank account details – is it from the usual contact and usual email address?

(b) Check the supplier history – have any other changes in standard data been requested, is this a supplier with high value transactions?

(c) Check letterhead to others from the same supplier and verify requests with trusted contacts at suppliers.

(d) At accounts department level, any modification in the particulars of suppliers, customers or any other business partners (especially bank details) should be independently checked by accounts department staff and confirmed with the customer/supplier concerned. Regarding bank details, only an original bank account identification form will be accepted.

(e) Ensure there is a periodic and frequent reconciliation of payments and accounts.

Continued >

4 Have the right payment controls in place

Use double signature/authorisation as an internal process

Double signature is preferable for any payment, or at least for payments above a certain amount. Ideally those having the authority to sign off payments will be divided into 2 groups, for instance 'A' (the necessary authority to commit the company) and 'B' (according to their function, and thus their capacity to validate a payment). The A+B combination ensures that all payments are duly cleared (A) and justified (B). Other combinations (A+A, B+B) should not be accepted.

- Make clear to your staff that they should err on the side of caution and should feel free to mention any suspicions (no matter how small) they have about a payment, financial transaction, payment change instruction to a designated senior member of your finance team.

Bank process

- The payment authority described above should be confirmed with your banks.
- Bankers must be asked to report, or even stop, any unusual transfer transaction (amount, beneficiaries, purpose, etc.). This recommendation applies in priority to 'manual' payments.

Payment methodology

- Secure means of payment must be favoured. For instance, electronic signatures (with biometric authentication for instance) are now offered by most financial intermediaries and can dissuade a person under influence or duress from being tempted to copy or reproduce a hand-written signature.
- Insecure payments (facsimile, paper, telephone, e-mail, cheques) if any should be limited and should always require a prior accounting entry.

5 Other key areas of consideration

- **Use of digital signature** - When internal e-mails are used to communicate important professional instructions, it is advisable to use digital signatures in e-mails. The company should always be in a position to authenticate incoming emails.
- **Whistle-blowing** – The procedure should be extended to situations in which company staff are threatened, intimidated or forced to act under duress by third parties, company managers or by authority figures (officer of the law, government officials, etc.).
- **Reception desks** should be told to treat unusual requests with caution. For instance, an unidentified call such as "Please put me through to the payments department" must be treated with caution.
- **Logistics** - Any modification in the method and/or place of delivery or collection should be authenticated with the external party concerned
- **Social Media** - All staff must be made aware of the risk posed by social media, which has become a fantastic source of information for fraudsters. The company should issue security instructions to staff, banning posting professional (and above all confidential) particulars on social networks. Furthermore, membership of a network groups (for example the 'Chief Financial Officers' group) is an additional risk; these groups are easy targets for fraudsters.
- **Website Protection** - Protection of the company's web site must be stepped up to guard against the risk of pharming [1]. Several technical measures should be considered: using a secure DNS protocol, or running web searches for sites having a DNS that is identical or similar to the company's. Preferably, this task will be outsourced to a specialist firm.
- **Involve the police** - In the event of attacks, the company must press charges forthwith.

[1] Pharming is the redirection of visitors to a fraudulent web site that has the same 'look & feel' and/or the same domain name as the web site they are looking for.

AIG Europe S.A., Osvald Helmuths Vej 4, DK-2000 Frederiksberg, Danmark Tel.: (+45) 9137 5300 Fax.: (+45) 3311 3340

0513