Impersonation Fraud

Fraud Alert Guidance

The aim of this guidance is to raise awareness of attempts by outside third parties to trying to steal company funds through impersonation techniques.

1. Inform Staff

As a matter of priority, alert all those that could be targeted across all geographies of your organization and raise their awareness to this type of fraud; not just at the Finance function level but also all functions likely to be in contact with third parties. This means that the alert should be general in its distribution and it should 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) Do not give important instructions (payment or otherwise) by telephone or by e-mail. Only requests received in writing and on letterhead should be acted upon, with a "call back" to the person purporting to send the instruction to confirm authenticity. 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. Complete a thorough call history by keeping logs of unusual callers and requests so they can be referred to when taking calls.

(c) Escalate any notes 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 third-parties (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 against others from the same supplier and verify requests with trusted contacts at suppliers.

(d) At accounting department level, any modification in the particulars of suppliers, customers or any other business partners should be independently checked by accounting staff and confirmed with the customer/ supplier concerned. Regarding bank changes, only an original bank account identification form should 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/authorization as an internal process

Double signatures approval processes are preferred for any payment, or at least for payments above a certain amount and for manual payments. Ideally those having the authority to sign off on 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, or 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 favored. 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.
- Non-secure payments (facsimile, paper, telephone, e-mail, checks) 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**—The best practice is 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 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 should press charges.

[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 Bring on tomorrow

www.aig.com

06/15 SP1033B