Instances of attempted supplier fraud are on the increase, and as the fraudsters are becoming increasingly skilled in their ability to misappropriate funds from schools, academies, colleges, and universities, a review of internal procurement policies and procedures could prevent a major loss.

At the end of last year, we were made aware of two very significant cases of fraud. Both incidents occurred at FE colleges that were in the middle of major building projects, and both involved the electronic transfer of funds from the colleges to contractors. The details of each case are frighteningly similar and provide a sobering reminder of the rising risk of fraud.

Both colleges were contacted by fraudsters who pretended to represent contractors working at the colleges at the time. Each college was using a different contractor but the circumstances are so similar that they can be explained as one.

The fraudsters had researched the contractors, starting by taking basic details from one of the many hoardings and signs put up around the building works. Clearly, the fraudsters then undertook further, detailed research to gather information they needed to imitate the contractors, convincingly.

The colleges were at similar stages in their building works, which is to say that the majority of the work had been completed, and some monies were shortly to be passed to the contractors. Each one was contacted by someone purporting to be from the contractors, giving genuine names of individuals from the contracting firms.

The fraudsters advised that the contractors’ banking details had changed and that the next payment for works completed should be made to a new bank account — the details of which were then offered.

Regrettably, no further checks were made and payments were made totalling circa £2 million. By the time the mistakes were spotted, the money had been removed from the fraudsters’ bank accounts altogether.

Sadly the two FE colleges aren’t alone in being targeted by these sophisticated criminals and there have recently been attempts of supplier fraud at other schools and colleges. All schools and colleges are urged to remain vigilant when dealing with notifications of changes to bank account details from their suppliers, and, if necessary, to review their procedures for dealing with and verifying any changes.

ARE WE COVERED FOR SUPPLIER FRAUD?

Unfortunately this type of loss is not covered by a traditional portfolio of insurance policies. It is not a “theft” nor a “money” loss in the insurance sense as there has been no physical misappropriation of the funds. Even if you secure traditional fidelity guarantee insurance, this will only cover the dishonesty of your employees, not of external suppliers or those purporting to be external suppliers. Therefore, the risk of supplier fraud needs to be managed via appropriately robust policies and procedures.
WHAT IS SUPPLIER FRAUD?
Supplier fraud is when someone convinces you to change payment details, by purporting to be a supplier you make payments to, and then requests a payment be made to these new banking details. For example, construction companies who publicise their presence with advertising hoardings during building works are often targeted due to the visibility of the commercial relationship and the nature of the payment schedules within the construction industry.

HOW ARE THE DETAILS OF SUPPLIERS OBTAINED BY FRAUDSTERS?
• Research of the supplier’s website to understand their activities and identify key staff.
• Press releases announcing the appointment of suppliers or the winning of specific contracts.
• Online transparency of tenders and the award of contracts.
• Unsuspecting employees tricked into providing details; this may include telephoning companies to gain information about their procedures or payment processes.

NOTIFICATION OF A CHANGE OF BANK DETAILS – THE FRAUDSTERS APPROACH
• Fraudsters may telephone with a change of bank details, often targeting junior or inexperienced employees who may be more likely to accept these changes.
• A written request on forged letterhead quoting publicly available information such as company registration and director details.
• An email request – just because the domain names match, doesn’t mean it is a legitimate email address, as fraudsters may have the ability to create electronic “aliases” or “clone” domain names.

HOW TO MANAGE THE RISKS OF SUPPLIER FRAUD
• Train and educate staff on an ongoing basis to ensure the potential dangers of providing sensitive company information, by phone or other means, especially contract and account information.
• Introduce a rigorous change of supplier details procedure – establish with your suppliers, and internally, procedures and points of contact for handling and changing sensitive information.
• When calling a supplier back to check the veracity of a request, always use details in your system, rather than those on any associated letter or email.
• If you are concerned about the source of a call, ask the caller to provide you with a main switchboard number for you to be routed back to them.
• A periodic review of suppliers should also be undertaken to identify and remove any old/dormant accounts from your finance system. This reduces the likelihood of any old supplier information being used to secure fraudulent payments, as only current, known suppliers will be active on the system.
• Ensure IT security controls are in place to help further mitigate the risk of any supplier fraud attempts.

USEFUL RESOURCES:
http://content.met.police.uk/Article/Mandate-fraud/1400013159214/1400013159214
http://www.actionfraud.police.uk/home

For further information on the insurance products and risk advisory services available to you, or if you would like to arrange a meeting to discuss your insurance requirements, please contact us:
☎ 01444 313100
✉ development.team@marsh.com
➡ uk.marsh.com/education

Join the Marsh UK Education Forum.