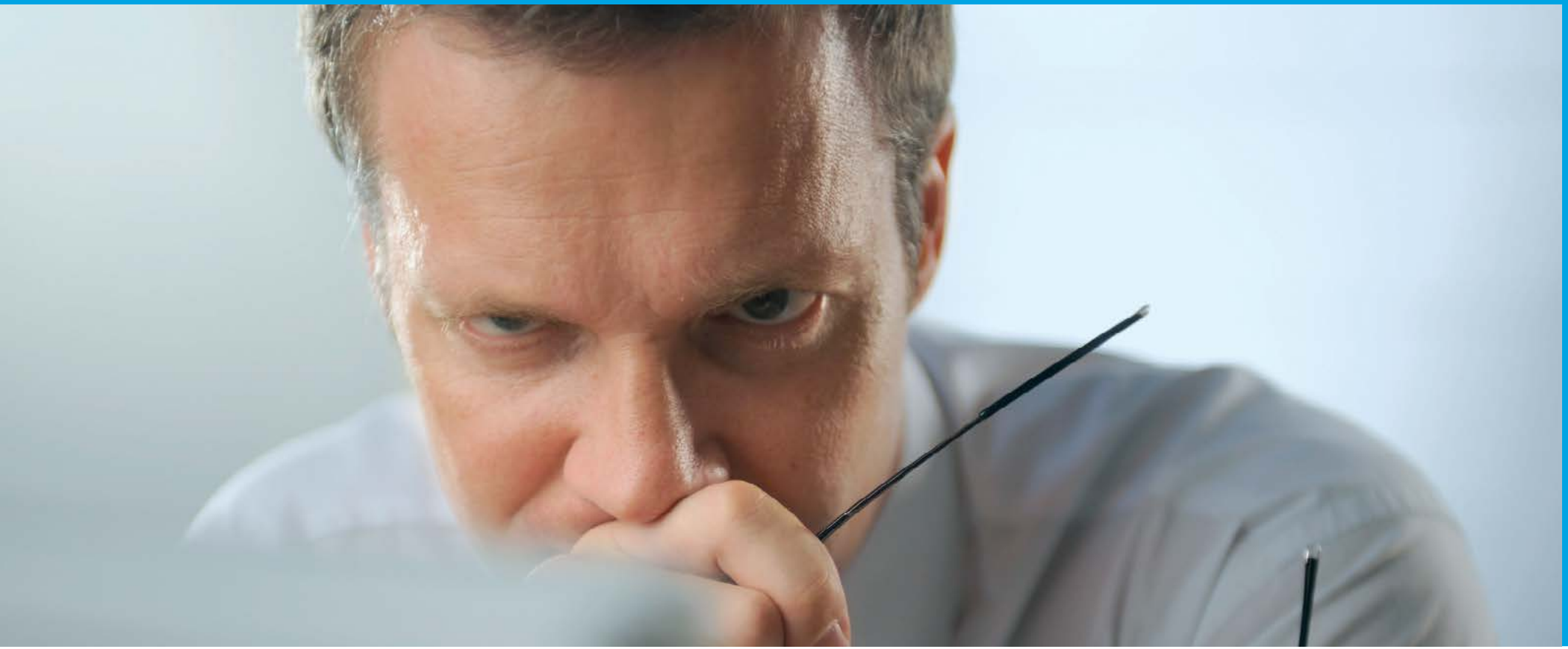


Fraud Illustrations and Scenarios

AIG

Fraud Illustrations and Scenarios

The following scenarios are intended to help illustrate the wide potential for fraud in day to day business activities. To try and make them clear and readable many of the scenarios in this note are presented as follows:

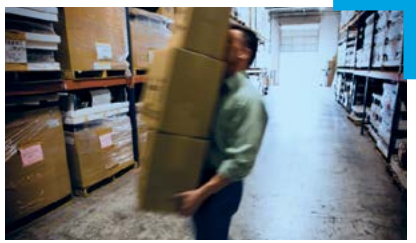
Opportunity
An outline of the fraud including the perpetrators' position and the industrial sector

Concealment
How the perpetrators concealed their fraudulent actions and avoided detection

Discovery
How the fraud was eventually discovered

Comment
Some comments and observations of our own about the scenario, based on our experience of underwriting crime insurance and handling claims.

We hope you find the material helpful and informative. Please feel free to share, print off, or email any of this information to colleagues or clients, and if you would like any further information about crime insurance, contact the financial lines team at your nearest AIG office (contact details can be found at the end of this document).



Fraud by lone employees

Fraud by collusion

Fraud by external attack

Fraud by lone employees

CLICK BELOW

01 Failure to segregate duties in the finance department

02 Excessive access for IT Manager

03 Vulnerable commission structure

04 Circumventing transfer authorisation procedures

05 Cashier's theft of incoming cash

06 Theft by Stock Manager

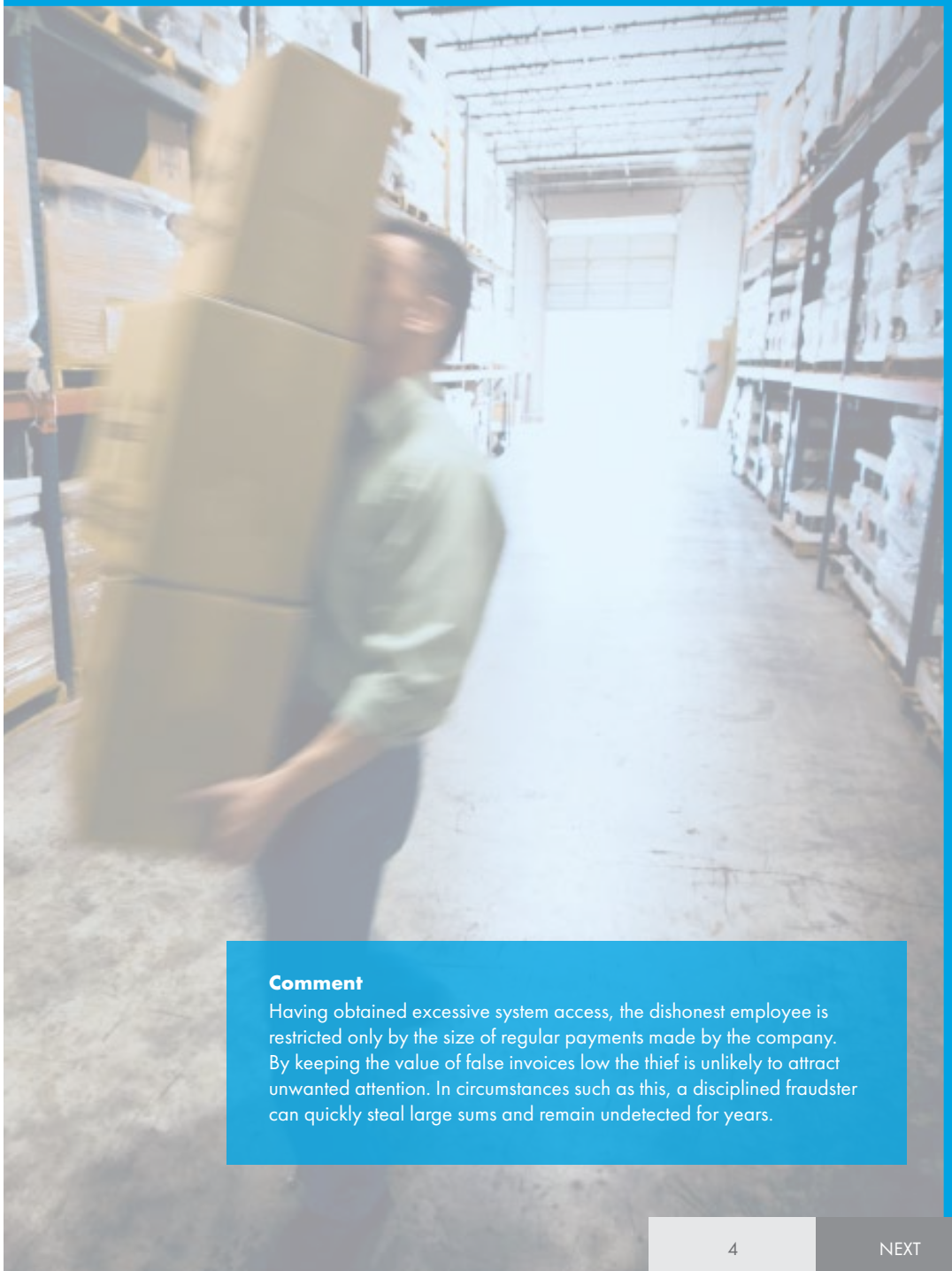
Failure to segregate duties in the finance department

01 Lone employee

Opportunity
To cover staff shortage an employee who processes invoices is also given access to the supplier creation system. This is not withdrawn when the regular staff return to work. The employee sees that when invoices are approved for payment, the financial controller examines the largest payment in detail and then signs the rest. The employee spots an opportunity to create and make payments to a false supplier.

Concealment
The employee creates an imaginary packaging supplier and submits a false invoice for payment. To his delight the payment is authorised and received in his bank account a few days later. The employee begins to submit similar invoices on a regular basis.

Discovery
The activity is uncovered during a routine supplier review when packaging costs are examined. It is revealed that over nine months, tens of thousands of pounds have been stolen.



Comment
Having obtained excessive system access, the dishonest employee is restricted only by the size of regular payments made by the company. By keeping the value of false invoices low the thief is unlikely to attract unwanted attention. In circumstances such as this, a disciplined fraudster can quickly steal large sums and remain undetected for years.

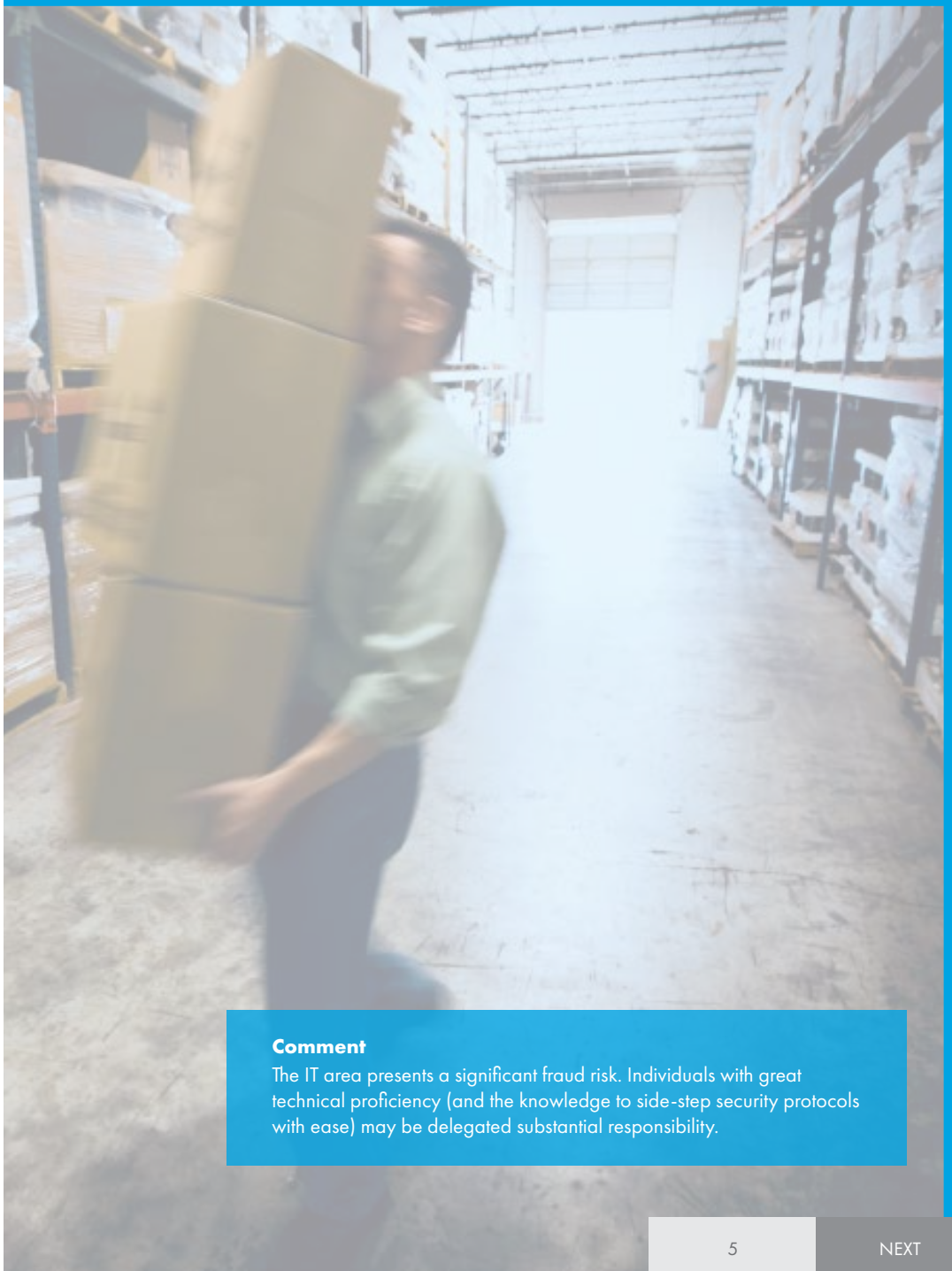
Excessive access for IT Manager

02 Lone employee

Opportunity
In a rapidly expanding company, the IT manager has full, unrestricted access to the company's systems, including the company bank account details. Having worked draining hours over the previous couple of years the manager is passed over in favour of an external candidate for an expected promotion to Chief Operating Officer. The manager decides to exploit his inside information, knowledge of passwords and procedures for his own benefit.

Concealment
The manager uses privileged systems information to divert company funds to his own bank account and conceals the fraud within the general ledger. On two occasions where queries arise, he tells the accounts department that the issue is due to a 'system imbalance' and promises to have it rectified as soon as possible.

Discovery
The fraud is uncovered as part of the testing at year end external audit. Unbeknown to the IT manager, the company's audit committee requests a full systems review to identify the cause of 'system imbalances'. The extent of the IT manager's fraud took several months to ascertain, such was the skill with which the account balances had been manipulated.



Comment
The IT area presents a significant fraud risk. Individuals with great technical proficiency (and the knowledge to side-step security protocols with ease) may be delegated substantial responsibility.

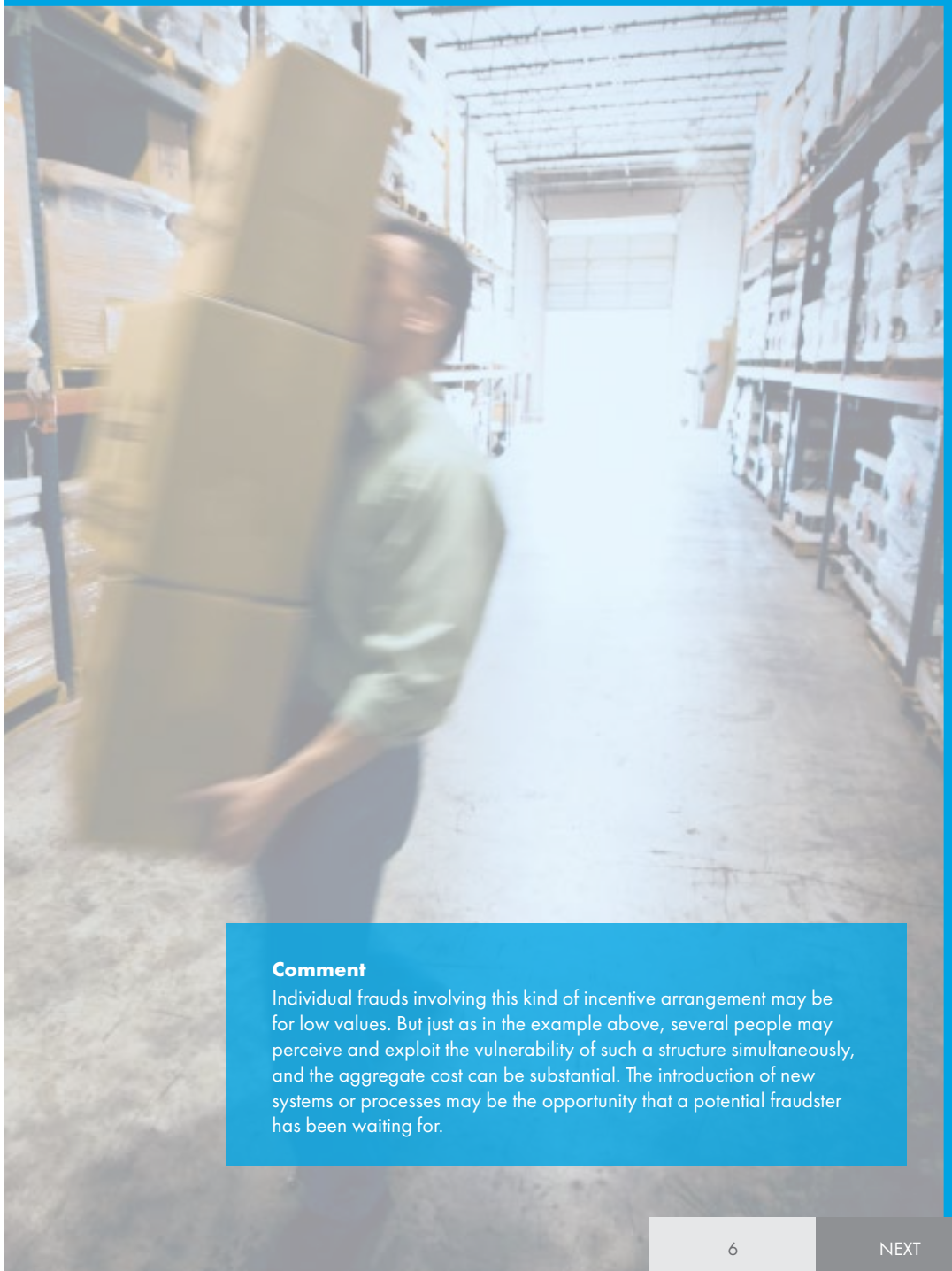
Vulnerable commission structure

03 Lone employee

Opportunity
To motivate its sales team, a company introduces a new commission scheme of six months' clients fees up front for each sale, with no clawback for cancellations. A member of the team is quick to exploit the new commission structure.

Concealment
The employee creates false sales to imaginary clients with fictitious names and addresses. He receives the commission relating to the new client and when payment for the sale is due, he uses some of his commission to make an initial payment before submitting a cancellation form from the client.

Discovery
The employee is able to develop the scheme for several months, which only unravels when low client retention levels attract attention. An investigation reveals that several members of the sales team are involved in similar activities.



Comment
Individual frauds involving this kind of incentive arrangement may be for low values. But just as in the example above, several people may perceive and exploit the vulnerability of such a structure simultaneously, and the aggregate cost can be substantial. The introduction of new systems or processes may be the opportunity that a potential fraudster has been waiting for.

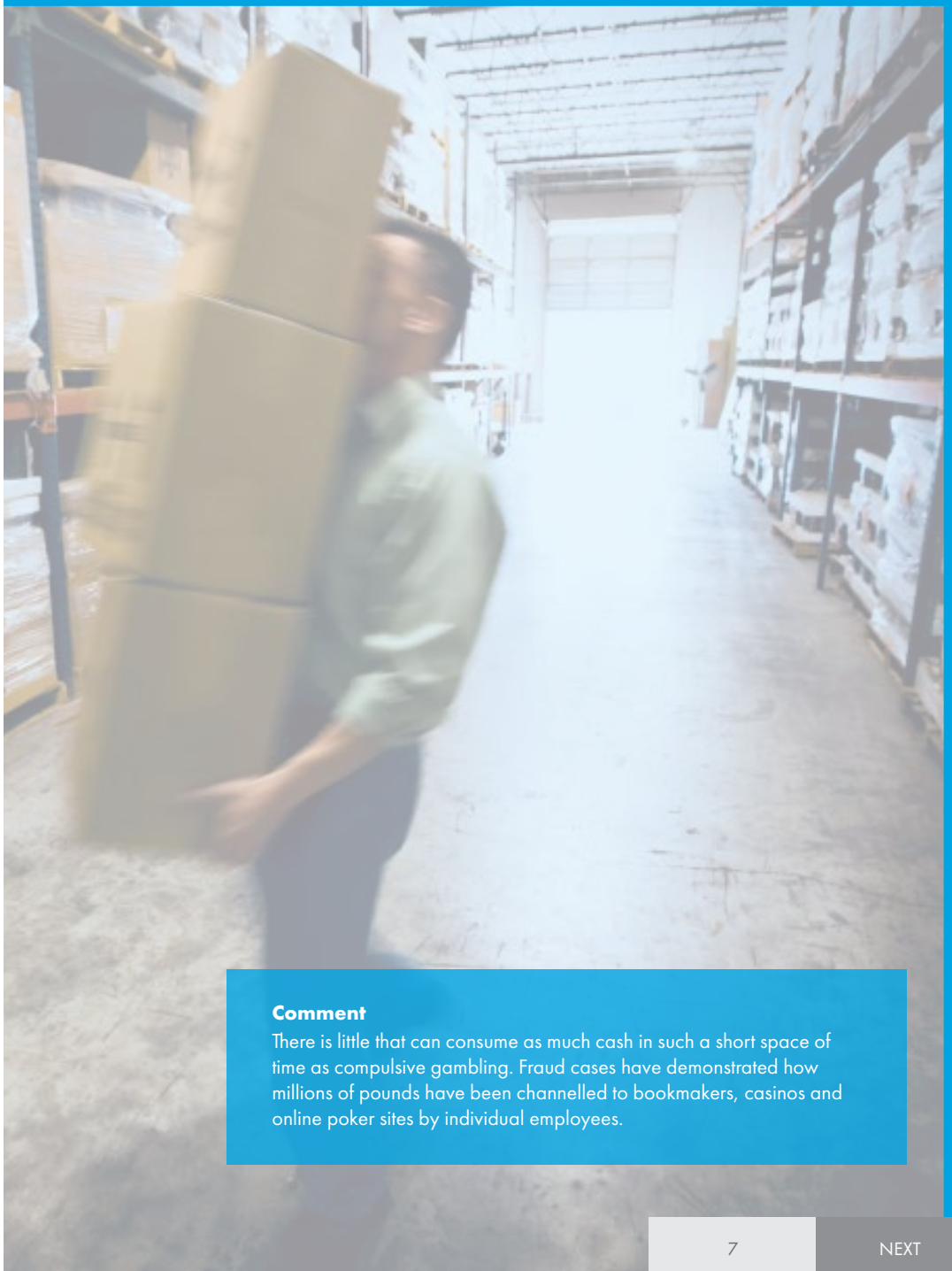
Circumventing transfer authorisation procedures

04 Lone employee

Opportunity
A finance manager struggling with gambling debt observes how the routine sharing of passwords among staff gives him an opportunity to approve, authorise and divert funds to his own account.

Concealment
By using a member of his department's password, the manager is able to generate refund payments to customers. He has the personal authority to approve and authorise these payments and he experiments by risking a small refund to his own bank account. With no one else involved in the authorisation process this was successfully completed. As the months progress the amounts and frequency of these transactions increase to substantial levels.

Discovery
The fraud is uncovered when the Finance Director queries the level of refunds, which in turn leads to an investigation and inevitably, discovery. Although the sharing of passwords is strictly prohibited by internal procedures, the investigation shows that the practice is commonplace.



Comment
There is little that can consume as much cash in such a short space of time as compulsive gambling. Fraud cases have demonstrated how millions of pounds have been channelled to bookmakers, casinos and online poker sites by individual employees.

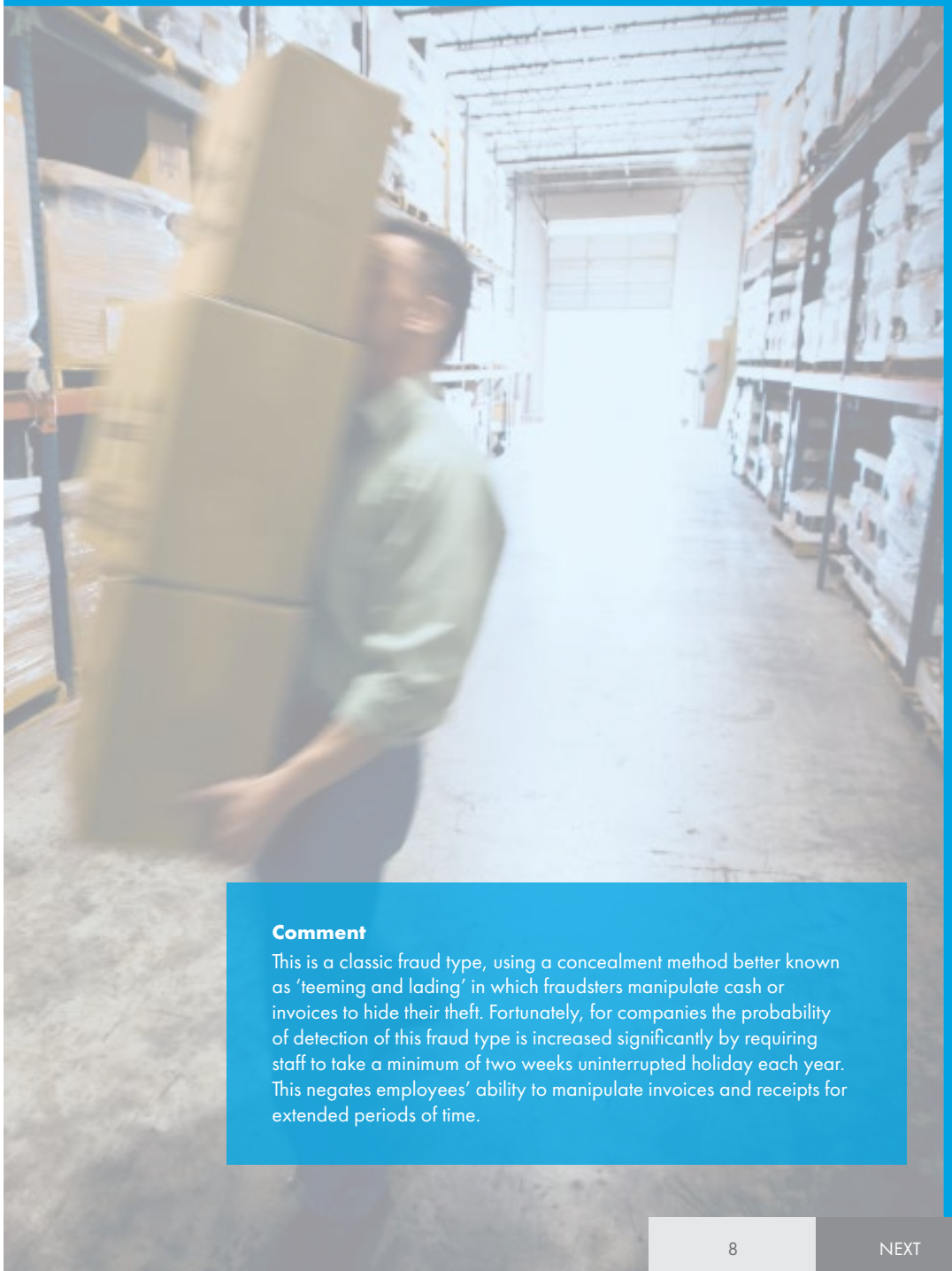
Cashier's theft of incoming cash

05 Lone employee

Opportunity
A team of cashiers handling tens of thousands of pounds each day is responsible for accepting client payments. One cashier observes that not all clients request a receipt and that accounts with frequent numbers of payments provide an opportunity for "manipulation".

Concealment
The cashier notes those clients with significant activity who are less diligent requesting receipts for their payments. The cashier starts to pocket a small percentage of the funds that should have been allocated to clients' accounts. If a receipt is requested then the cashier simply waits for another potential target.

Discovery
The cashier is able to successfully continue the fraud for several months. The scheme is uncovered by the company when a client complains, having received a statement, that several large payment settlements have not been allocated to their account.



Comment
This is a classic fraud type, using a concealment method better known as 'teeming and lading' in which fraudsters manipulate cash or invoices to hide their theft. Fortunately, for companies the probability of detection of this fraud type is increased significantly by requiring staff to take a minimum of two weeks uninterrupted holiday each year. This negates employees' ability to manipulate invoices and receipts for extended periods of time.

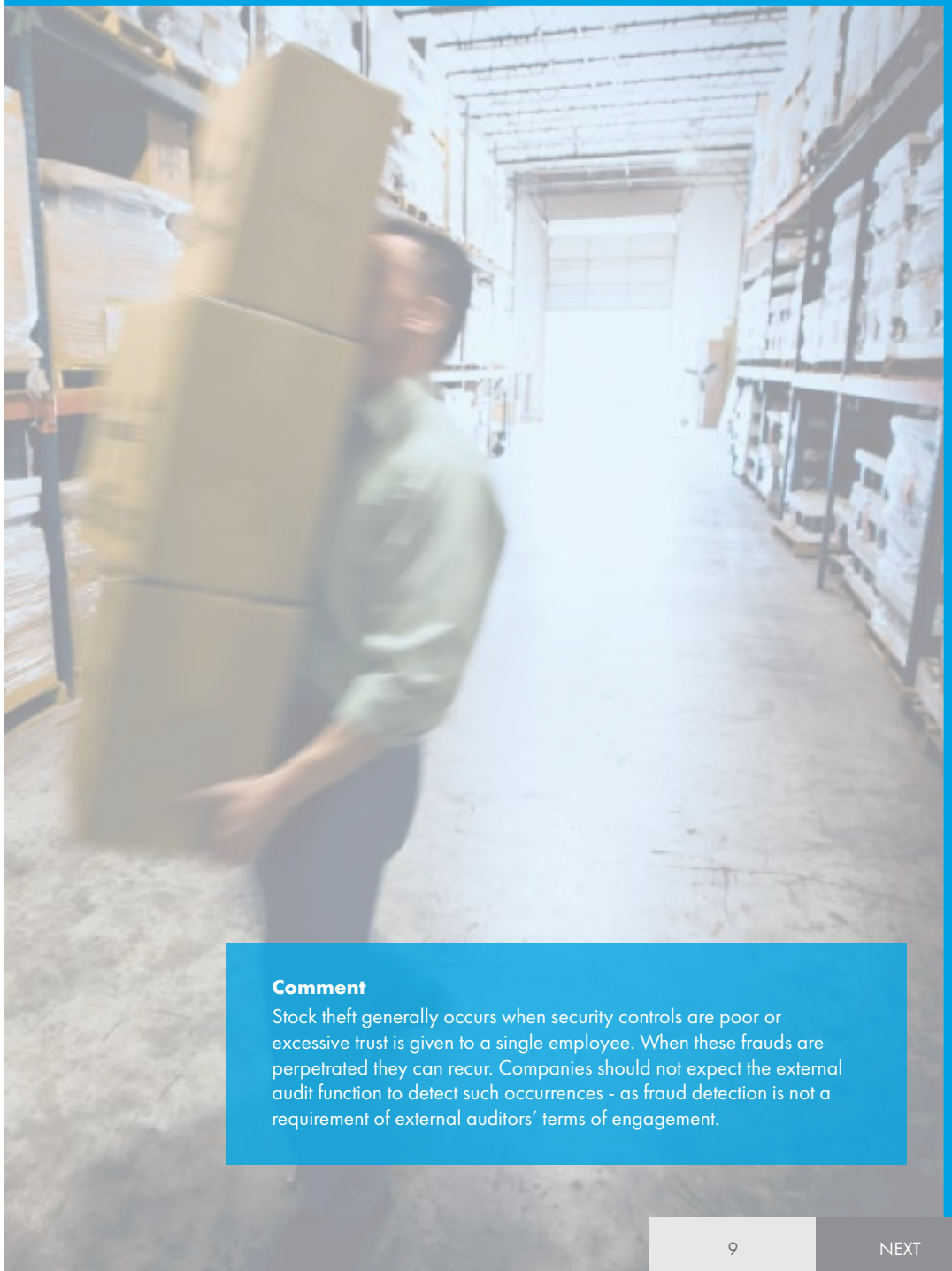
Lone employee: theft by stock manager

06 Lone employee

Opportunity
A respected and trusted manager of twenty years service has responsibility for all stock related matters and general security. For several years he has been making full use of the opportunity to abuse his privileged position by stealing stock.

Concealment
The manger manipulates goods received notes, by deleting them, amending them or simply losing them to ensure that the fraud went undiscovered. He simply loads the stolen stock into his car on Friday afternoons when there are few people around.

Discovery
The fraud is discovered when the external auditors complain about the stock manager's record keeping and demand an improvement. As the papers are tidied up many discrepancies in the stock records come to light and the manager eventually confesses to his activities. Although the weekly sums stolen were relatively small, the cumulative effect over many years was significant.



Comment
Stock theft generally occurs when security controls are poor or excessive trust is given to a single employee. When these frauds are perpetrated they can recur. Companies should not expect the external audit function to detect such occurrences - as fraud detection is not a requirement of external auditors' terms of engagement.

Fraud by collusion

CLICK BELOW

01 Discretionary discount scheme
02 Weak stock procedures
03 Kickbacks for contract allocation
04 Manipulation of temporary staff numbers
05 Remote office fraud
06 Personal expenses abuse

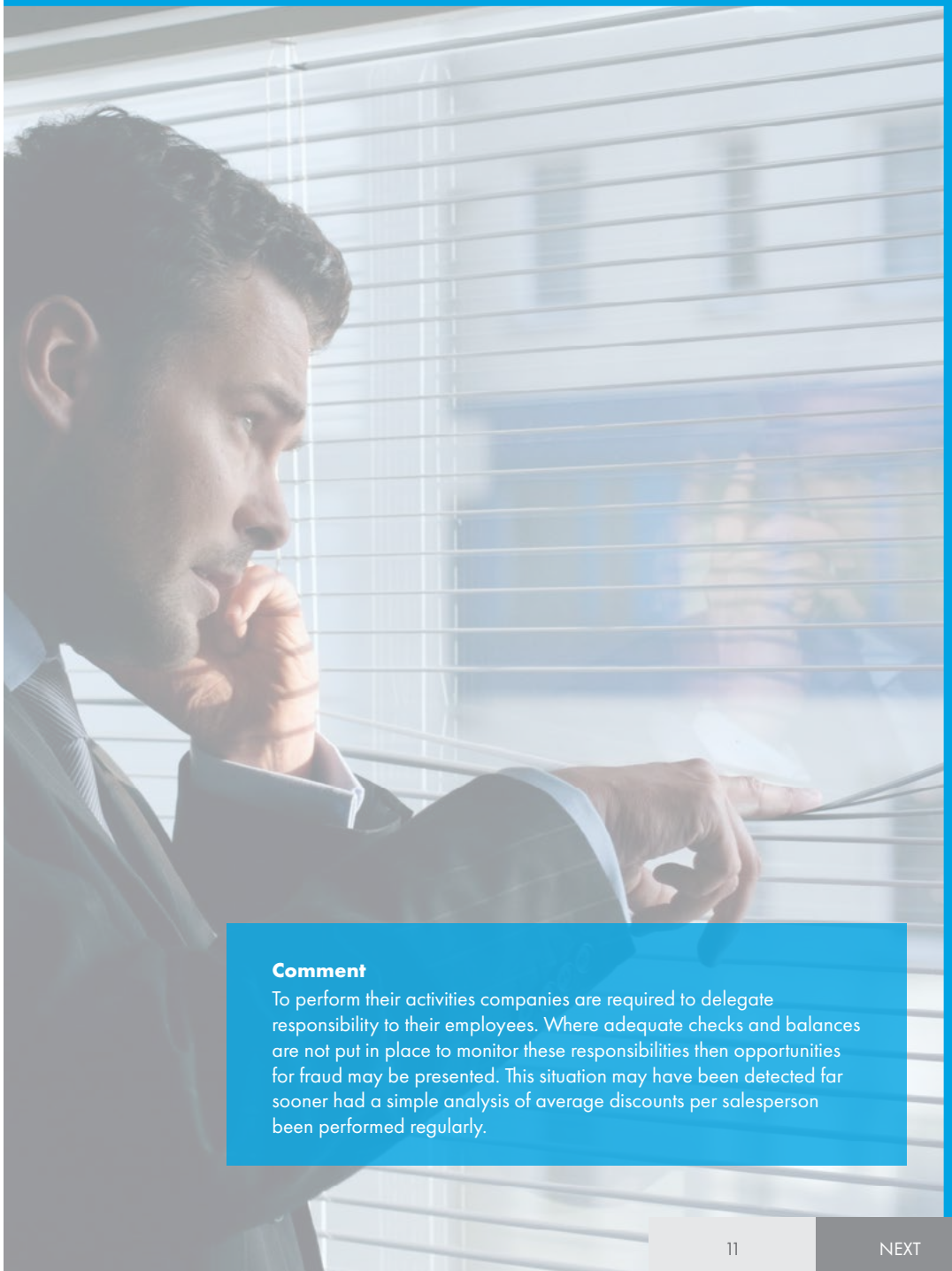
Discretionary discount scheme

01 Collusion

Opportunity
The members of a small sales team are empowered to negotiate prices with clients with discretionary discounts of up to 20%. Discounts are to be reported to head office and applied to the client's invoice. A team member spots an opportunity to take advantage of this process.

Concealment
The employee approaches three of his closest clients and explains that their current discounts of 5% can be potentially quadrupled, on the understanding that the additional discount is split between the client and the sales person. The clients agree and begin to receive 20% discounts on all sales, with the salesman pocketing a cash equivalent of 7.5%.

Discovery
The fraud continues for almost two years before detection when a work colleague comments to a line manager that a member of the sales team must have been doing very well to have purchased a top of the range sports car. The manager makes some discreet enquiries which increase suspicion, before questioning the employee who owns up to the scheme.



Comment
To perform their activities companies are required to delegate responsibility to their employees. Where adequate checks and balances are not put in place to monitor these responsibilities then opportunities for fraud may be presented. This situation may have been detected far sooner had a simple analysis of average discounts per salesperson been performed regularly.

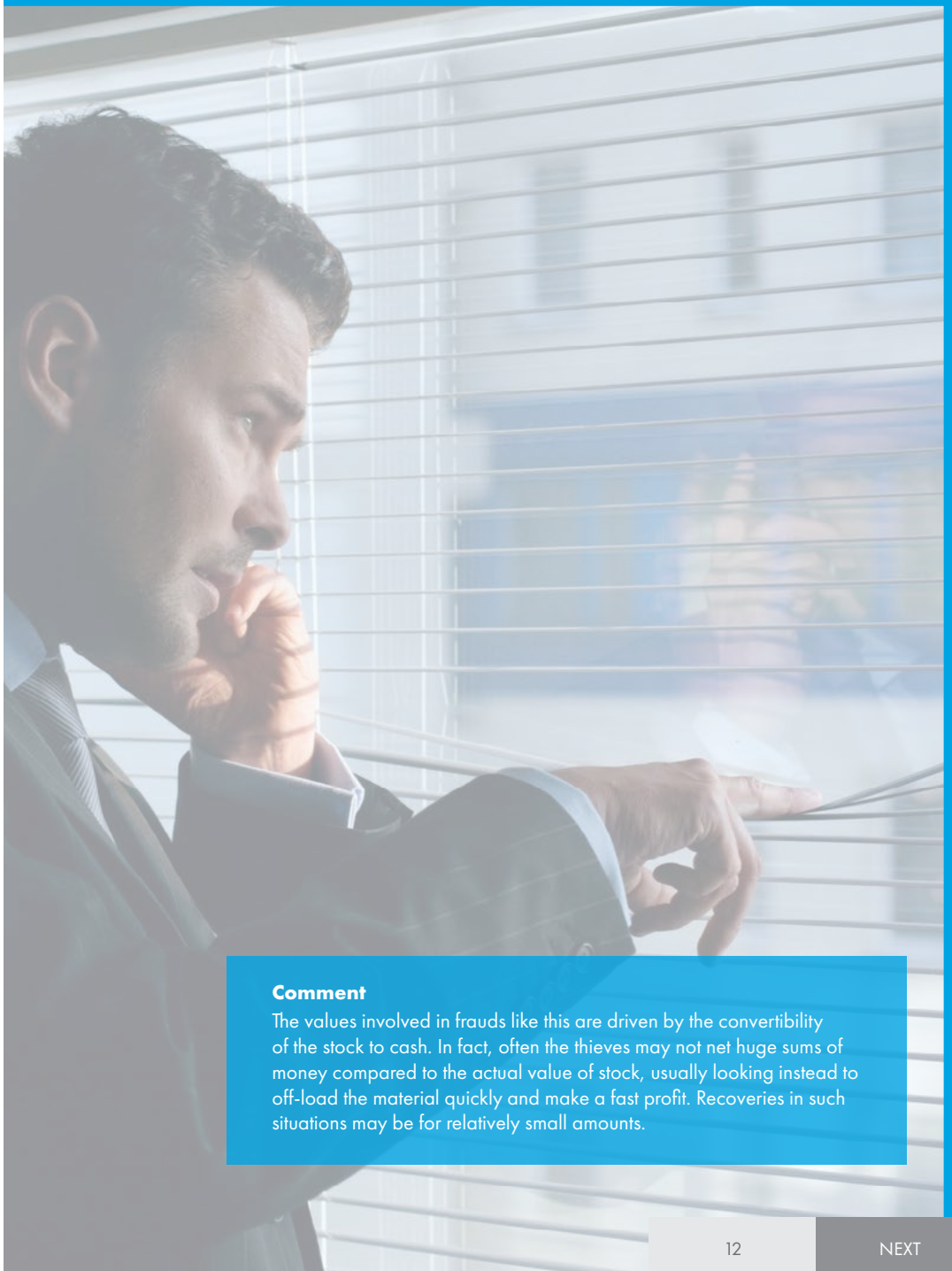
Weak stock procedures

02 Collusion

Opportunity
A member of the quality control team is friends with the company's stock manager. Discussing their responsibilities in the plant they recognise that controls over damaged stock are lax with crates of damaged items abandoned in a corner of a warehouse. Disposal procedures are haphazard. They see a profitable opportunity to work together.

Concealment
The quality controller labels undamaged products as substandard, indicating that they need to be returned to the factory for disposal. At the factory the complicit stock manager packs the goods for destruction, prepares the necessary documentation and arranges for the "faulty" stock to be removed from the premises. The stock is then sold off in pubs and Internet auction sites at a large discount, for a healthy profit.

Discovery
The scheme is uncovered when another company employee, is in one of the bars when the stock is being sold, and anonymously, tips off the company. An internal investigation shows that over £100,000 of stock has been stolen. The company recovers £5,000.



Comment
The values involved in frauds like this are driven by the convertibility of the stock to cash. In fact, often the thieves may not net huge sums of money compared to the actual value of stock, usually looking instead to off-load the material quickly and make a fast profit. Recoveries in such situations may be for relatively small amounts.

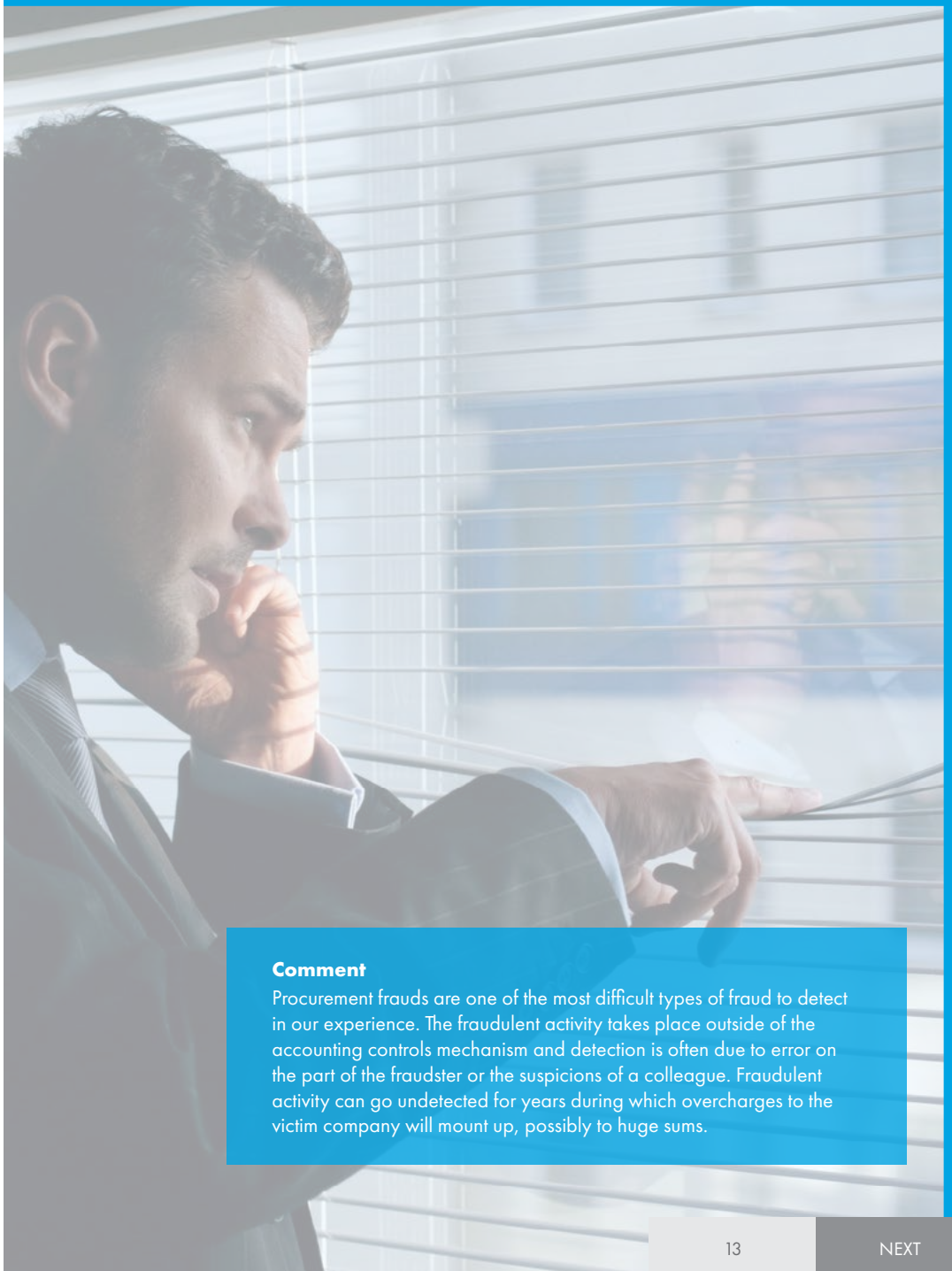
Kickbacks for contract allocation

03 Collusion

Opportunity
An employee has responsibility for recommending suppliers of raw materials to senior management. This employee has a long record with the company, is well trusted and his recommendations are invariably accepted by management - a situation that also presents an opportunity for preference and fraud.

Concealment
Unbeknown to management, one significant supplier provides an all-expenses paid holiday each year to the employee for the recommendation. The supplier then submits (successful) bids that are some 15% higher than competing tenders.

Discovery
This fraud is only uncovered after an error by the fraudster, who one evening boasts to colleagues about his luxurious holidays and the source of his next trip to the Caribbean. This was promptly reported to management who discovered that the arrangement had been in place for the last twelve years.



Comment
Procurement frauds are one of the most difficult types of fraud to detect in our experience. The fraudulent activity takes place outside of the accounting controls mechanism and detection is often due to error on the part of the fraudster or the suspicions of a colleague. Fraudulent activity can go undetected for years during which overcharges to the victim company will mount up, possibly to huge sums.

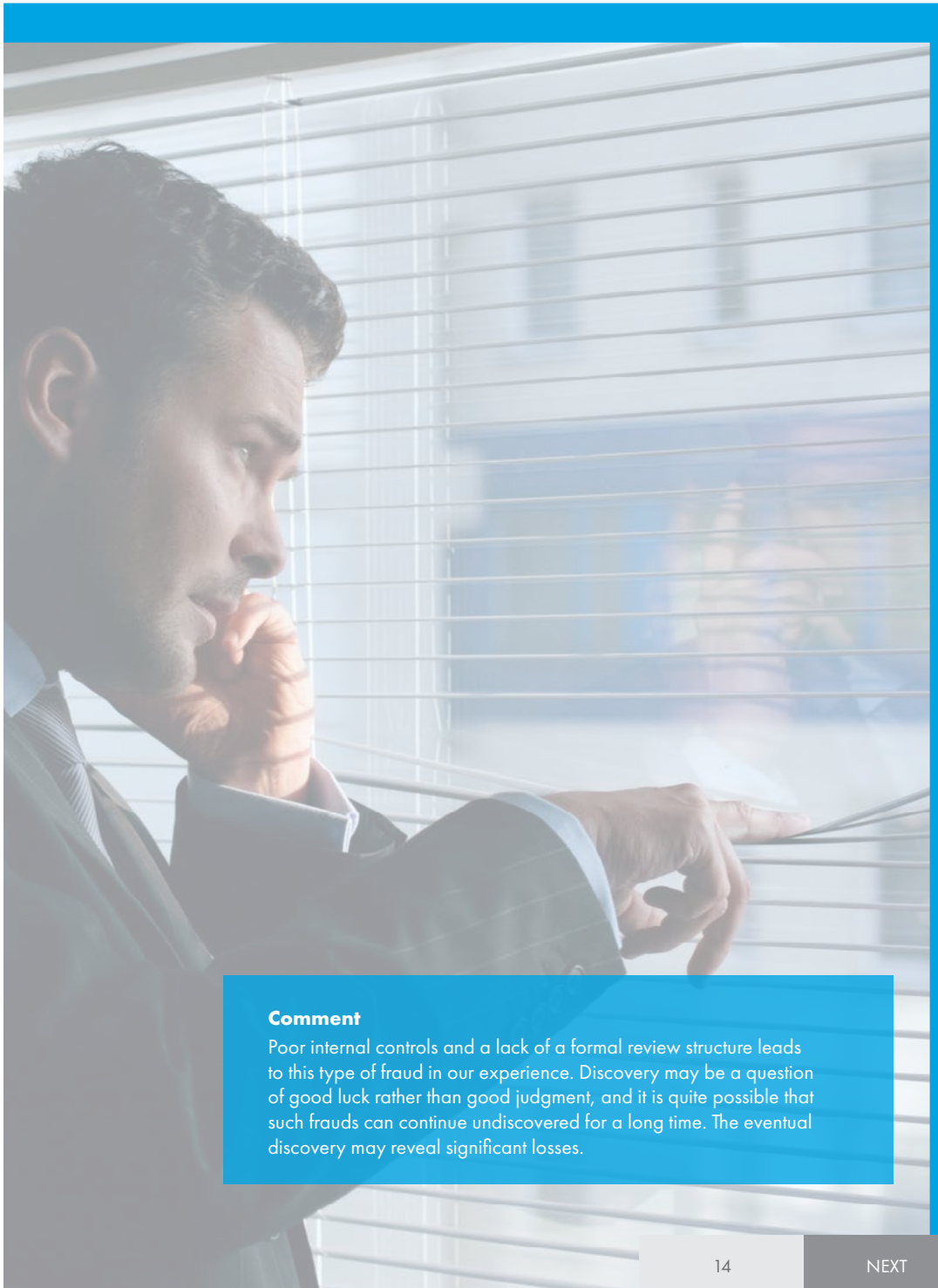
Manipulation of temporary staff numbers

04 Collusion

Opportunity
Temporary members of staff are paid weekly. The payroll clerk responsible for the payroll run has a sister working for the employment agency that provides the temporary staff. There is no review of the payroll run and after an accidental error in reconciling staff numbers from the agency one week, the sisters see an opportunity to manipulate staff numbers for their benefit.

Concealment
Each week one sister invoices the company for several temps that do not exist. The payroll clerk authorises these as genuine employees and these 'employees' are paid each week directly to the sister's bank account. This continues for over a year netting a sizeable sum for the fraudsters.

Discovery
The fraud is exposed when the payroll clerk is suddenly taken ill on payday. When the replacement begins to prepare the weekly payroll it immediately becomes apparent that there are several unaccounted employees and the scheme quickly unravels.



Comment
Poor internal controls and a lack of a formal review structure leads to this type of fraud in our experience. Discovery may be a question of good luck rather than good judgment, and it is quite possible that such frauds can continue undiscovered for a long time. The eventual discovery may reveal significant losses.

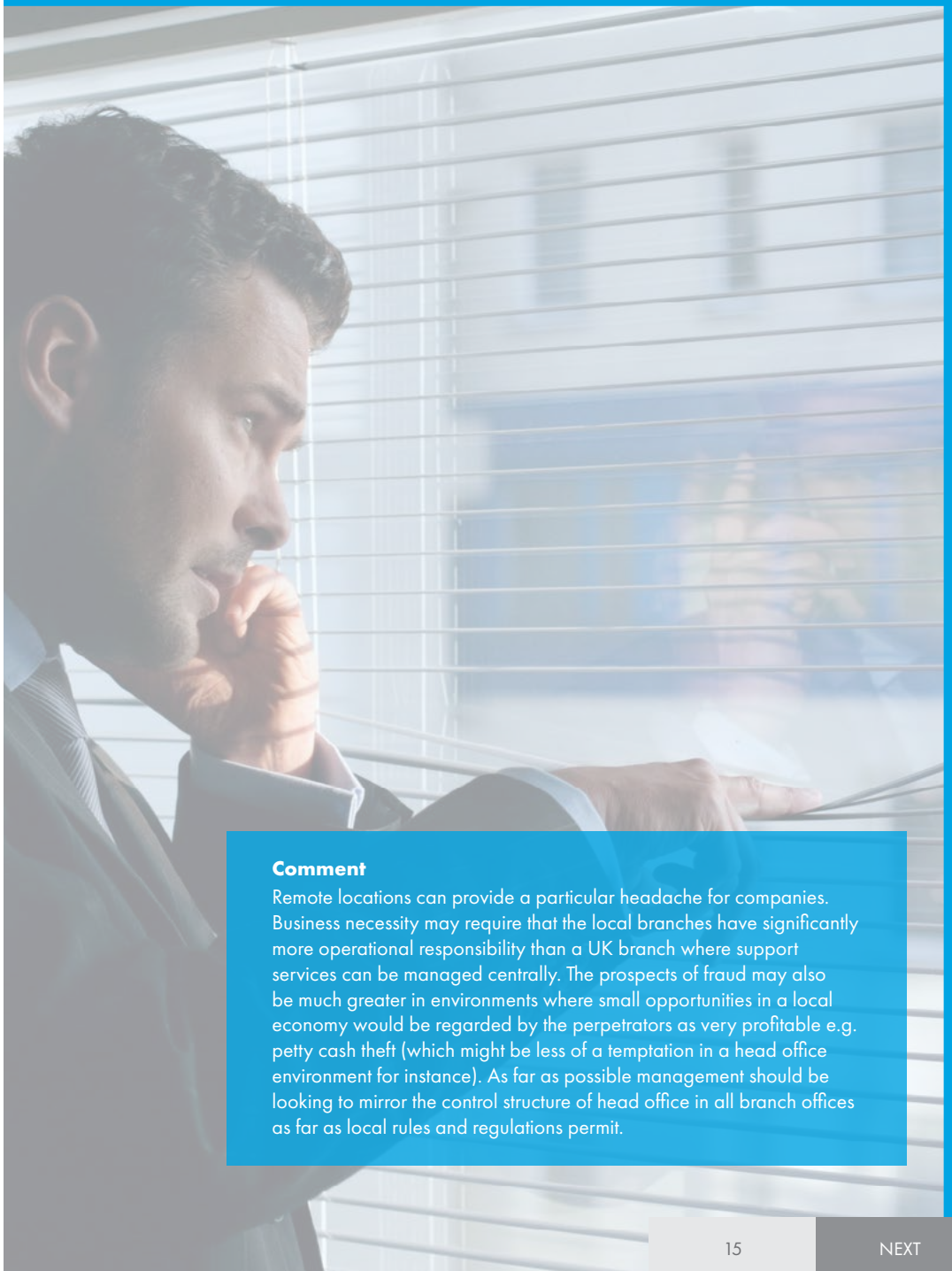
Remote office fraud

05 Collusion

Opportunity
A small branch office in West Africa operates with two employees who have absolute control over all branch activities. The branch always shows a profit but does not contribute large sums to the group's profit worldwide. Political instability discourages internal audit visits for several years. The two members of staff see the opportunity to operate the company for their own benefit.

Concealment
Concealment is not difficult. Provided that the quarterly reported profit figures are within 5% of that period's budget, no further questions are asked by head office.

Discovery
The fraud is discovered when the financial controller is unable to get in contact with the branch for several weeks. This finally prompts an internal audit visit which reveals that the office had been unoccupied for at least six weeks. The responsible individuals had been stealing the profits for months before leaving the company for good.



Comment
Remote locations can provide a particular headache for companies. Business necessity may require that the local branches have significantly more operational responsibility than a UK branch where support services can be managed centrally. The prospects of fraud may also be much greater in environments where small opportunities in a local economy would be regarded by the perpetrators as very profitable e.g. petty cash theft (which might be less of a temptation in a head office environment for instance). As far as possible management should be looking to mirror the control structure of head office in all branch offices as far as local rules and regulations permit.

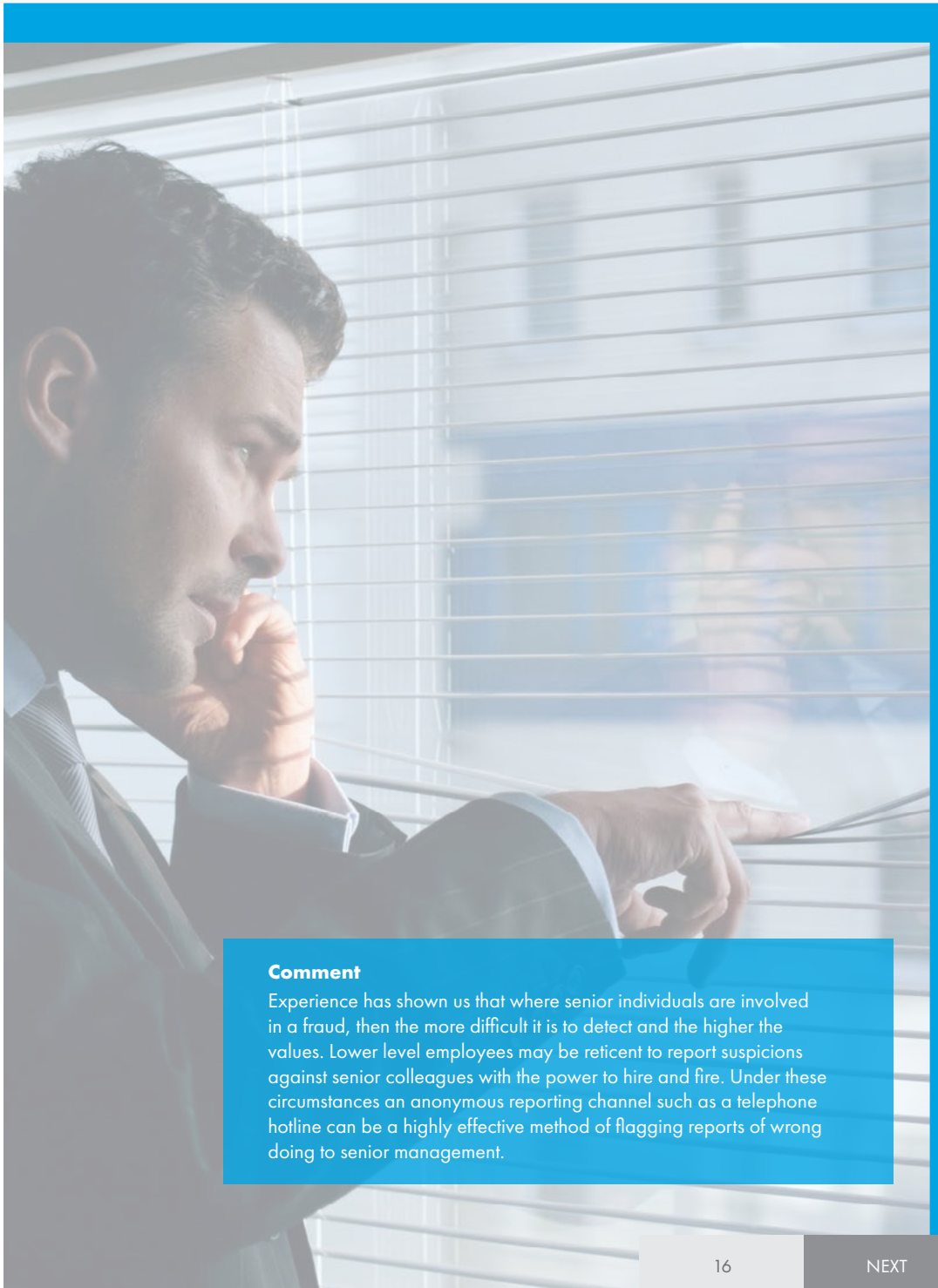
Personal expenses abuse

06 Collusion

Opportunity
A company's sales and finance directors have worked together for a company for over 15 years. They are good friends and regularly socialise outside of work. After one expensive night out with their respective partners the sales director suggests they charge the meal to their company's account. They later discuss and refine a procedure for making the most of such opportunities.

Concealment
The sales director is required to have his expenses signed off by the finance director, who complies, knowing that it was fraudulent. After doing this several times for dinners, the partnership begins to step up its activities to include corporate gifts and luxury items. The fraud continues for several years, helped by the individuals' seniority within the company which allows them to continue stealing unchallenged.

Discovery
The fraud is uncovered when a recently appointed personal assistant sees what's happening and sends an anonymous email to the company vice-president. The resulting investigation uncovered high levels of fraudulent expenses including charges for a helicopter and boat charter.



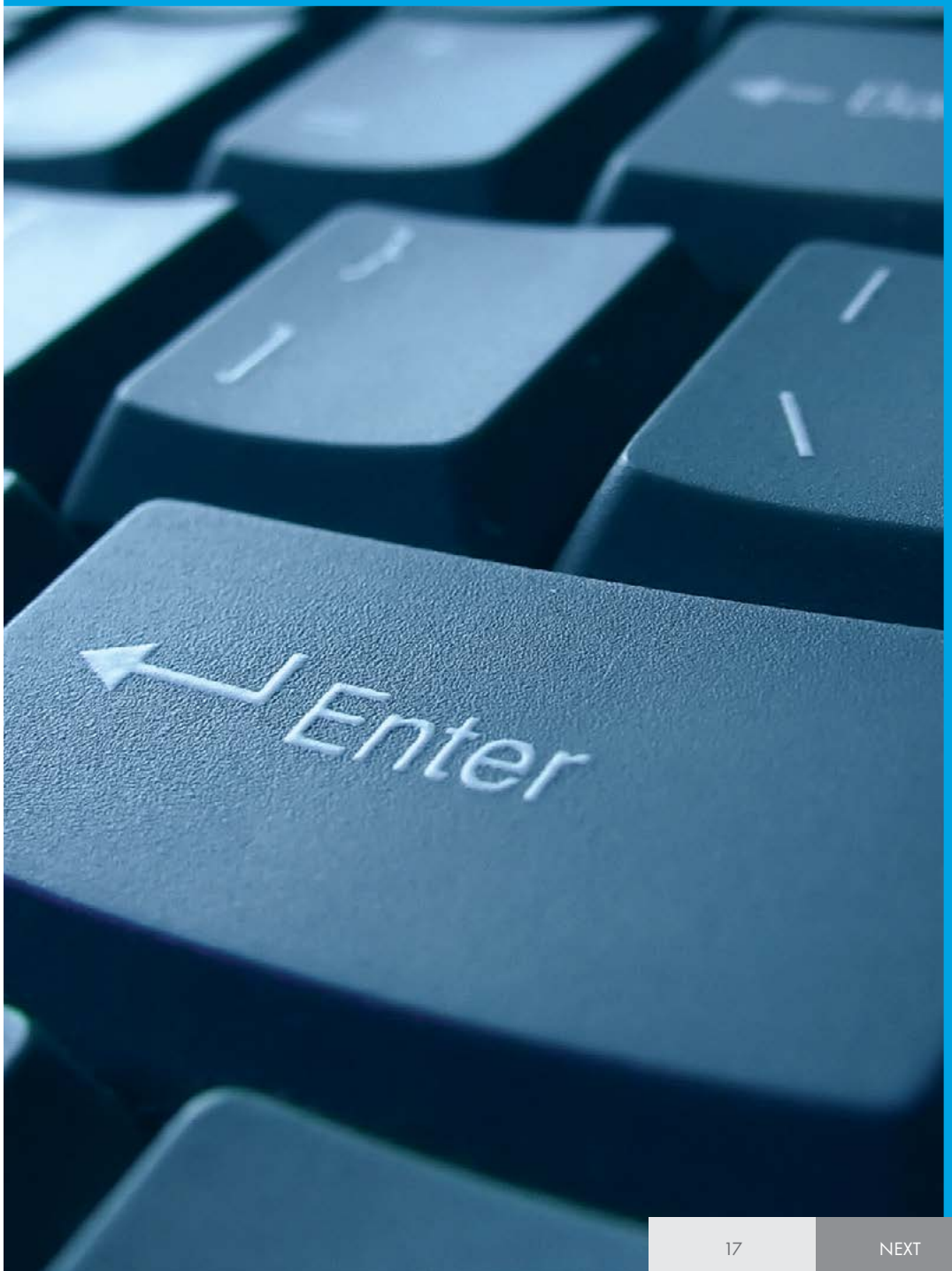
Comment
Experience has shown us that where senior individuals are involved in a fraud, then the more difficult it is to detect and the higher the values. Lower level employees may be reticent to report suspicions against senior colleagues with the power to hire and fire. Under these circumstances an anonymous reporting channel such as a telephone hotline can be a highly effective method of flagging reports of wrong doing to senior management.

Fraud and external attack

CLICK BELOW

01 Forged fax transfer

02 Hacking into company systems



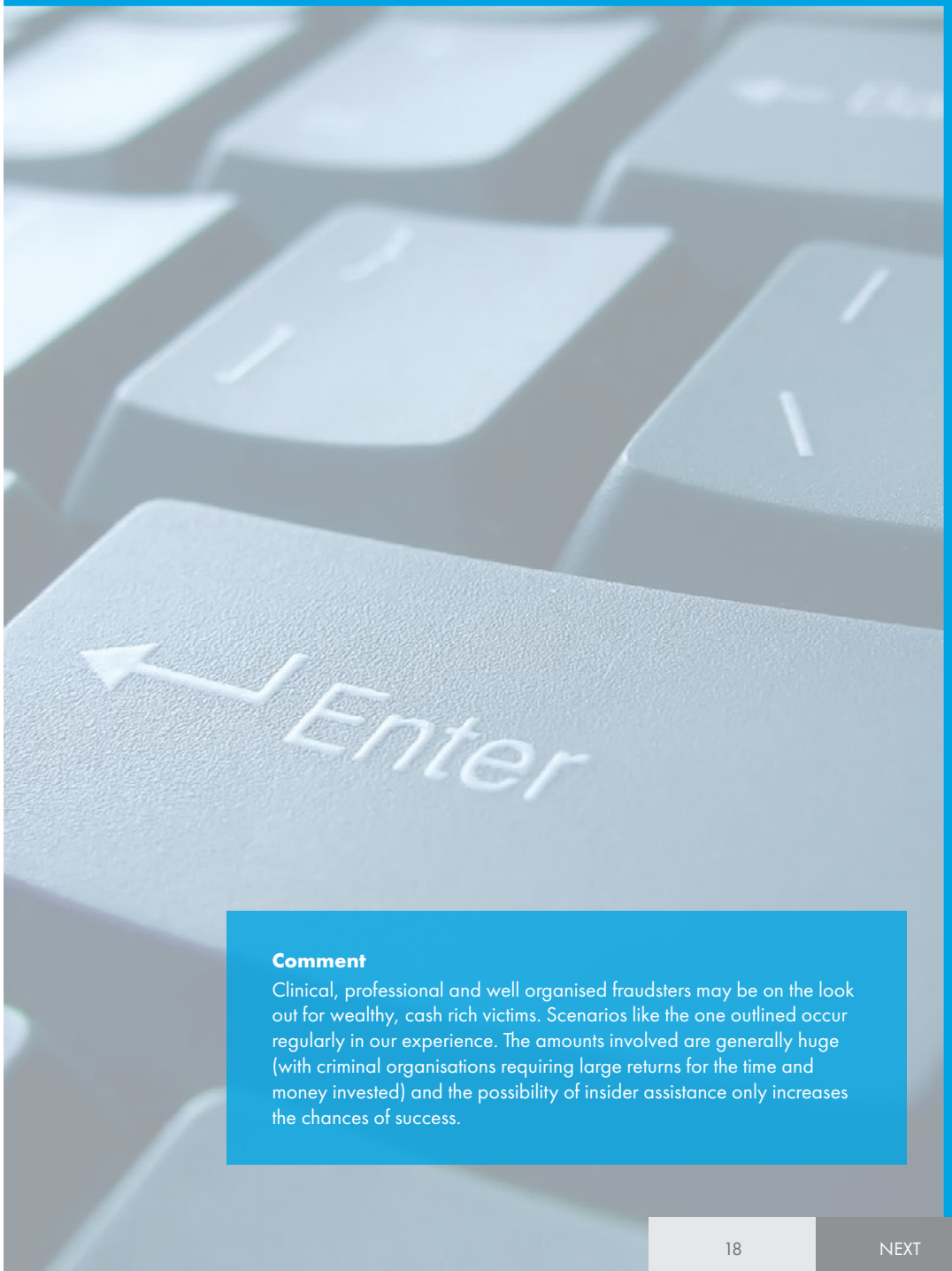
Forged fax transfer

01 External attack

The Attack

During a review of transfer activity, a company's financial controller is shocked to find that a seven figure sum has been transferred to an offshore bank account. It is discovered that a forged fax transfer had been accepted by their bankers. The fax contained signatures matching those on the mandate agreed between the bank and the company, which is why the bank, in good faith, had accepted the forged instrument and performed the transfer.

The subsequent investigation suggested that the transfer could have been performed with the collusion of staff but there was no proof that employees had been involved. The stolen funds proved impossible to trace as, immediately upon transfer, the funds had been moved between multiple financial institutions.



Comment

Clinical, professional and well organised fraudsters may be on the look out for wealthy, cash rich victims. Scenarios like the one outlined occur regularly in our experience. The amounts involved are generally huge (with criminal organisations requiring large returns for the time and money invested) and the possibility of insider assistance only increases the chances of success.

Hacking into company systems

02 External attack

The Attack

Two members of staff in the finance department have password protected responsibility for the on-line electronic fund transfers from the company's bank accounts. One morning an attempt to make a payment to the company's suppliers is greeted with an error message. The staff contact the bank's technical support and are informed that the bank is unable to make payment as the company accounts are showing almost zero balances. An urgent investigation is launched and it transpires that earlier that day an individual had hacked the on-line system and emptied the company accounts. The monies were transferred to off-shore bank accounts with the amounts being quickly removed and deposited elsewhere.

Comment

System intrusion via cyber crime continues to grow and develop in skill and complexity as technology advances and the fraudsters become more sophisticated. Criminals can defraud companies remotely from their laptops.

www.aig.co.uk

BELFAST
Enterprise House
55/59 Adelaide Street
Belfast BT2 8FE
Tel: 02890 726002
Fax: 02890 726085

BIRMINGHAM
Embassy House
60 Church Street
Birmingham B3 2DJ
Tel: 0121 236 9471
Fax: 0121 233 3597

CROYDON
2-8 Altyre Road
Croydon
Surrey CR9 2LG
Tel: 020 8681 2556
Fax: 020 8680 7158

GLASGOW
4th Floor
69 Wellington Street
Glasgow G2 6HJ
Tel: 0141 303 4400
Fax: 0141 303 4440

LEEDS
Yorkshire House
Greek Street
Leeds LS1 5SX
Tel: 0113 242 1177
Fax: 0113 242 1746

LONDON
58 Fenchurch Street
London
EC3M 4AB
Tel: 020 7954 7000
Fax: 020 7954 7001

MANCHESTER
4th Floor,
201 Deansgate
Manchester M3 3NW
Tel: 0161 832 8521
Fax: 0161 832 0149

GBL97734 FLS CRI Dec 18