Commercial Crime: Claims Scenarios

- Internal Crime cover is provided as standard, External Crime cover is elective. Where both are purchased, the cover forms an 'all risks' crime policy. Note therefore that loss scenarios below are not named perils, merely circumstances which might give rise to a loss by virtue of the wide cover provided under policy.
- This provides a synopsis only, to provide a brief explanation. For full terms, conditions, exceptions and details of any sub-limits applicable please refer to the Schedule and policy wording.
- Whilst many of these claims scenarios have been based on real life examples from the press or experienced by our own customers, details have been amended to protect the identities of the companies involved or elaborated for the purposes of illustrating the cover.

Insuring Clause or Extension	Loss Scenario	Claims Example
Internal Crime	Payroll fraud by an employee.	Two employees working in the HR department of a large public sector company colluded in setting up a 'ghost' employee on the payroll. One of these employees was more senior, able to authorise the payment runs and was responsible for reconciling the records. They paid the fictional employee a salary of £85,000 annually and then would split the proceeds. This fraud was discovered five years later, when the loss totalled £425,000.
Internal Crime	Theft of stock/equipment by an employee.	Over a 3 year period, an IT manager working for an energy company bought computer equipment in their employer's name, worth £19m. The equipment was purchased from a single supplier and delivered either to the IT manager's home or a storage unit before he sold it at a fraction of the true value, to small businesses or individuals bidding on an online auction site. The re-sale proceeds were used to fund a gambling addiction.
Internal Crime	Theft of funds by an employee.	A procurement manager at a shipping company duped their employers into believing she had won lucrative contracts with two major clients. The company delegated the responsibility of £250,000 worth of funds to the manager believing she was using the money to pay workers to carry out these new contracts. In reality she was using the stolen funds to buy her new partner high value gifts and going on exotic holidays. Upon discovery of the fraud she was unable to repay the funds as these had been spent and had no other assets.
External Crime	An insured relies on a forged signature, instruction or counterfeit negotiable instrument (for example a bank note) and in doing so suffers direct financial loss.	An employee working in the accounts department of a manufacturing company received a letter from a regular supplier asking for their bank account details to be changed on their payment system. The request was made on legitimate-looking headed paper with logos and included a forged signature. The letter provided the insured with a telephone number, offering them the opportunity to 'verify' this request (meaning the employee rang the fraudster directly). Changes to the bank details were made and over the next couple of weeks, 3 payments totalling close to £400,000 were made to this new bank account. Discovery occurred when the legitimate supplier contacted the manufacturer asking why payments had been stopped. The money was never recovered.
External Crime	Cheque fraud i.e. loss due to forgery, counterfeiting or fraudulent alteration of cheques. This includes cheques made by the insured or cheques given to the insured in payment for goods or services rendered.	A small utilities company reimbursed a customer by cheque for an overpayment on their bills. The cheque was fraudulently altered by the customer who cashed the amended cheque, defrauding the utilities company by several thousands of pounds.

External Crime	Third parties illegally stealing property through cyber means.	A third party fraudster gained access to a pharmaceutical company's computer system by piggybacking on a sophisticated computer virus which enabled entry. The fraudster changed the distribution address of an order worth £58,000 and took delivery of the goods, never to be seen again.
External Crime	Third parties illegally stealing funds through cyber means.	A housing association received a (genuine looking) email with an attachment which purported to have been sent by HMRC. This was opened by an employee in the accounts department which infected the insured's computer system with malware, enabling third party fraudsters to access the employee's system and transfer over £250,000 from their bank account. By the time the illegal intrusion was discovered the money had long since disappeared. There was virus protection in place, but it was not sufficient to protect against such a sophisticated Trojan virus. The bank refused to accept liability for the loss, citing the fact it was the insured's system and not their own that had been compromised.
External Crime	Corporate card fraud - where corporate credit, debit or charge cards are stolen and used fraudulently by third parties.	A marketing company issued corporate cards to a number of their employees. On a night out an employee misplaced their wallet in a bar. Mistakenly believing that he would find it again, he did not notify the card issuer within the required 24 hour period. When he did notify the loss a week later, he discovered that a thief had used his corporate card to buy goods on the internet. As the marketing company had not complied with the terms and conditions of the card issuer, they were liable for these costs, value of loss £17,000.
Automatic Cover Extension (1) – Expenses	This extension is designed to pick up costs and expenses following a loss ('after-care'), including costs for: • paying qualified professionals to quantify a Loss (investigation costs) • defending the insured against any legal proceedings following a loss • paying public relations consultancy fees to minimise adverse publicity following a loss • mitigation costs where insured has taken action to reduce or minimise a loss • costs relating to reinstating data (where damaged/destroyed/erased/stolen) • costs for replacing/repairing damage to the insured's premises or any furnishings & fixtures, safe, vault or cash box.	A nationally recognised charity's counter-fraud head submitted false invoices for 'intelligence investigations' from bogus companies, to the value of over £60,000. The employee's role ensured they were naturally a trusted member of staff and the invoices were not questioned for some time. The scheme was discovered after an internal inquiry was launched to investigate allegations that the employee had behaved unprofessionally and the legitimacy of the invoices were queried and professionally examined (investigation costs). The charity's reputation suffered considerable damage through extensive and negative media reporting; it was necessary to neutralise this as soon as possible to ensure public donation income did not suffer (public relations consultancy fees).
Automatic Cover Extension (2) – Care, Custody and Control & Client Loss	This extension is designed to protect an insured against loss of money, securities or property that does not belong to an insured but where they are legally liable and it is in their care, custody and control.	A gift box manufacturer won a substantial contract with an upmarket cosmetics company. They had been employed to design the packaging of a line of their perfumes and aftershaves. They took delivery of several large pallets of the cosmetic company's stock, worth over £350,000. Three of the company's employees managed to steal a substantial amount of this stock, despite stringent physical security. The gift box designer was liable to repay the cosmetics company for this loss as per the terms of their contract with them.

Automatic Cover Extension (3) – Corporate Identity Fraud	This extension is designed to indemnify the insured for costs & expenses incurred through reinstating the insured's own public records that have been fraudulently modified, stolen or altered. Cover also extends to include legal costs sustained where the insured has had to apply for legal proceedings to be dismissed on the grounds that there has been a corporate identity fraud. Finally, the insured is indemnified for costs relating to the hiring of a private investigation agency to identify the perpetrator of such a corporate identity fraud.	A criminal gang targeted a management consultancy company by informing Companies House of changes to the company's details. Companies House were informed that new directors had been appointed and the registered office address had changed. The gang then approached a different company, an office equipment distributor, purporting to be directors of the management consultancy and made a large order on credit. The order was delivered to the fraudulent address where the gang received the goods. The office equipment distributor tried to take the management consultancy to court when they refused to pay for the goods. The management consultant had to hire lawyers to argue that a corporate identity fraud had taken place and they were not liable to the third party. The insured then hired a private investigation agency to try to determine who had perpetrated the fraud.
Automatic Cover Extension (4) – Discovery Period	If the policy is not renewed and the policyholder doesn't buy a similar insurance elsewhere, then we will indemnify the insured following expiry of their period of insurance for loss that was sustained during that expired period of insurance which would have been picked up when the policy was in force, but which was discovered up to 90 days afterwards.	A professional services company had purchased commercial crime insurance for ten years. They had been claims free during this time and the financial director made a decision to lapse the policy at renewal to make savings on their insurance budget. Six weeks following the lapse of the policy an employee fraud was discovered, to the value of £120,000 which had been perpetrated throughout the previous 6 years and which would have been covered by the expired policy. The discovery period allowed the insured to make a valid claim against the policy for the loss sustained during the time that the company was on cover.
Automatic Cover Extension (5) – Acquisitions During the Period of Insurance	In recognising the fact that companies are frequently changing their corporate structures and creating or acquiring new companies, our policy automatically extends cover to indemnify a new Subsidiary Company or Associated Company which is created/ acquired during the period of insurance.	Halfway through their period of insurance, a large council set up a marketing company to promote tourism in their area. One of these new employees colluded with a company supplying publishing services who authorised inflated invoices and then shared the inflated profits with that employee. It was not necessary for the council to declare this creation to us as it satisfied the requirements of the policy conditions and therefore was automatically insured.
Automatic Cover Extension (6) – Interest Payable or Receivable	Calculated using the Bank of England base rate averages, this section indemnifies the insured for loss of interest that would have accumulated but for the fraud being perpetrated.	An employee fraud spanning 5 years was perpetrated against a hotel group. The total loss equated to £465,000 over this period of time. In addition to the direct financial loss sustained, the hotel group also lost out on interest that would have been payable on this amount.
Automatic Cover Extension (7) – Court Attendance & Staff Disruption Costs	Employee and third party frauds can sometimes turn into complicated legal battles, which can result in employees spending significant business time in meetings with legal personnel or authorities.	Following a loss of client funds due to employee dishonesty, an advertising company was taken to court over a disparity regarding the value of the funds missing. Several partners and employees were required to attend the legal proceedings as witnesses over a significant period of time, meaning they were unable to carry out the usual duties for which they were remunerated, at a substantial cost to the business.
Automatic Cover Extension (8) – Contractual Penalties	This extension caters for eventualities where the insured is required to pay contractual penalties as a result of a loss under the Policy.	A secondary school hired some high value visual effects equipment for a school production. The school's contract with the equipment company specified that the equipment must be returned by an agreed date or their 25% upfront deposit would be forfeited. The equipment was stolen by an unidentified employee the evening before this was due to be returned. The school lost their deposit.

Automatic Cover Extension (9) – Business Interruption Costs	This extension is designed to protect an insured for circumstances when a covered loss has caused them additional costs and expenses (following an initial 48 hour Waiting Period) to restore the insured's normal course of operations. These expenses could relate to rental fees for hiring temporary premises, costs of employing additional workforce and / or transport costs for moving equipment.	A criminal diverted the electrical supply from a nearby conference centre business to heat the criminal's outdoor swimming pool. The discovery of this caused the company's building to be deemed unsafe and the site was evacuated. The company had commitments to customers so after the 48 hour Waiting Period temporary premises were rented and a removal firm hired to move their equipment to an alternative, safe location where business could resume. The costs and expenses incurred in making such arrangements were in the region of £13,500.
Automatic Cover Extension (10) – Benefit Schemes	We will indemnify an insured for direct financial loss sustained to any Benefit Scheme (including pension plans, share purchase schemes or health plans) that has been declared to us. The excess does not apply to this extension.	A publishing business had a longstanding benefit scheme in operation. The trustee of the scheme fraudulently siphoned off over £120,000 from this scheme over a period of several months to prop up a business venture in which he had invested. The trustee's business venture had subsequently failed so recovering the stolen funds was not possible and the company was liable to repay the monies to the scheme.
Automatic Cover Extension (11) – Malicious Damage to Data	We agree to cover the cost of reinstating electronic data if it was damaged, destroyed, erased or stolen by an employee or third party. We will also cover the costs of removing malicious code (i.e. unauthorised and harmful software code including viruses).	A third party hacked into the computer system of a double glazing company and their entire customer database was deleted. The majority of their new business leads came from this valuable data and therefore it was crucial that this was reinstated. Experts were hired to reinstate this information using specialist data retrieval software, at a cost of £8,000.
Automatic Cover Extension (12) – Impairment of Money and Securities	Where money or securities have inexplicably disappeared, been damaged/destroyed or been stolen on the insured's premises or in transit, this extension will pick up the exposure. It also protects money and securities stolen from the interior of any bank, post office or building society.	An employee working for a luxury food and drink retailer was taking the day's cash takings to the bank. Whilst waiting in the queue the employee was distracted by a couple having a loud argument next to them. This had been a deliberate ploy by a gang of criminals, where another individual took the opportunity to steal the money from the employee without them noticing. The bank's CCTV recorded the incident but the money was never recovered.
Automatic Cover Extension (13) – Outsource Service Provider Crime	This extension is designed to recognise that not all business functions are carried out 'in house'. The Employees of vetted third party companies who have been entrusted with the custody/access to money, securities or insured property are covered by the policy.	An aerospace company outsourced their payroll function to a reputable third party company. An employee at the Outsource Service Provider added several 'ghost' employees to the payment runs, in essence paying themselves several hundreds of pounds every month. The insured retained the right to audit this payroll company and vetted them for honesty prior to their appointment; notwithstanding this the fraud was perpetrated and caused the insured significant financial loss.
Automatic Cover Extension (14) – Erroneous Electronic Transfer of Money	This extension caters for the eventuality that funds are transferred to the incorrect account and cannot be recovered.	An employee set up a payment beneficiary for a new supplier and transferred £32,000 to this account. There had been an innocent error inputting the account number and the funds were therefore not paid into the intended account. Despite the fact the bank was cooperative in trying to recover the funds, these had already disappeared by the time the company had realised the error. No other recovery methods were available.

Automatic Cover Extension (15) – Recruitment Costs	The costs of recruiting a new member of staff can be significant. Where an employee has been dismissed as a result of an internal crime, this extension provides cover for costs associated with the recruitment of a replacement member of staff.	The IT manager working in the energy company in the internal crime example above was dismissed following the discovery of their fraud. The position vacated was of a senior level, paying a salary of £60,000. The recruitment fee was 25% of the replacement employee's annual salary.
Public Utilities Fraud - see Condition (15)	The policy provides cover for charges for which the insured is legally liable following the direct theft of gas, water and / or electricity by an employee or third party from the insured's premises. Note that where perpetrated by a third party the cover is sub-limited.	A leisure business received an unusually high electricity bill. The amount was queried by the company, who informed their electricity supplier that there was no reason why their expenditure should have increased. Upon investigation it was revealed that a third party had diverted some of the electrical supply into a neighbouring building for the purposes of growing illegal plants. The charges equated to over £12,000.
Telecommunications Fraud - see Condition (16)	The policy provides cover for charges which the insured is legally liable for when an employee or third party fraudulently uses an insured's telecommunications system. This could include systems used on the insured's premises or accessed remotely where a fraudster has hacked into the system. Note that where perpetrated by a third party the cover is sub-limited.	A dental practice experienced a high value telecommunications fraud over the course of a bank holiday weekend. A third party fraudster hacked the insured's telecommunications system and made a high volume of calls to a premium rate telephone number to which they were affiliated. The fraud was only discovered when the company received their monthly telephone bill and it was realised that the system had been compromised.