CLEAR
INSURANCE MANAGEMENT

10 examples of **Crime** claims

- A top-30 independent broker
- 17,000+ clients across sectors
- Chartered insurance broker - only 3% of UK brokers qualify
- Access to the best specialist insurers
- Dedicated in-house claims team

Many businesses choose not to arrange crime insurance, potentially exposing themselves to the devastating effects of fraud and theft. We recommend that businesses consider arranging crime insurance and to illustrate why, here are 10 examples of crime losses that have directly affected our clients:

1. Suppliers email hacked

A large UK construction corporation client purchased safety barriers from a supplier, which cost over £100,000. The supplier's IT systems were subsequently hacked and the fraudsters trawled through their recent business orders.

An invoice was then sent out from the supplier's correct email for the actual order value and our client paid it without checking the new bank details provided on the invoice. The bank details were those of the fraudster and the money was never recovered. No crime cover was in place for our client or their supplier and we believe negotiations are still ongoing as to who the loss will fall to.

This client was offered crime insurance both before and after the loss took place, but chose to change their systems as opposed to arranging insurance.

2. Fake email request for payment

At a very busy period around Christmas, the FD of a small family-run event management/marketing company client received an email from her husband requesting a payment of £22,000 for a supplier.

The email appeared to show the correct email address and the FD paid the amount requested without conducting their usual new account detail checks. It was only when a further request for a larger payment was made that the FD queried her husband and they discovered the fraud.

No crime insurance was in place to cover this loss and the client's former broker had not highlighted that this cover was available. We now arrange crime insurance for this client.

3. Complex contractor fraud

A recruitment consultant client was subject to a lengthy and complex fraud involving the placement of a temporary contractor. They received an email, purporting to be from the large shipping agent Kuhne Nagel (K+N), requesting a temporary assignment be undertaken.

K+N proceeded to request the services of a contractor they had used before for a similar job, who was based in the Far East. Our client checked out the contractors references and company and went forward with the 'contract'. They paid the contractor £25,000 of fees for the work they believed had been carried out. When they subsequently sent their invoice to 'K+N' they were

advised that the order had never been placed. We believe K+N advised that they were aware of similar frauds being conducted against other recruitment firms.

We had offered this client both crime and cyber prior renewal, but the FD confirmed in writing that crime insurance was not required.

4. Fake president fraud

The FD of a large interior design client, turning over around £80,000,000, paid three invoices totaling £225,000 without checking the supplier bank details. The invoices were fraudulent and the money was sent to the perpetrator's accounts in Czech Republic.

Luckily there were multiple frauds being undertaken and £150,000 of the client's payments were held when the accounts were frozen. Whilst the client has lost £70,000 it is hoped that the remainder will be returned in full.

5. Fraudulent notification of change of supplier bank details

Our client's accounts department received an email from a prestigious customer of theirs (or so they believed). The email stated that the receiving bank account details had changed so could they please send the monies owed to a new bank account, for which the details were provided.

Unsuspecting of anything underhand at play, our client made payment. A few days later they received a legitimate chaser from their customer for payment. It was at this point they realised something was amiss. On further investigation, the fraud was detected. Unfortunately, by this point, the receiving account had been closed and the money withdrawn.

6. Theft of cash by site manager

Another client operated a temporary summer site that ran for six weeks only. The manager in charge was taking money from the safe after all other staff had left the site. Over a short period, he stole circa £90,000 to feed a gambling addiction. Initial concerns were raised when head office flagged that June sales had not been entered onto their accounting system. It was then noticed that our client's bank had only received one weeks' takings from the event.

Our client's expectation at this point was that the takings would still be in the safe. However, when checked, the safe only contained £3,658 leaving an amount of £92,299.68 unaccounted for.

7. Employee system breach and theft

An employee / employees of a client obtained passwords to the till computer system that they were not authorised to have. They used these to access the system and delete transactions from the days takings. They then took cash to the value of the deleted transactions so that the till 'balanced'. The irregular pattern of deleted transactions was picked up and investigations ensued, which led to the full extent of the loss being discovered (circa £50K).

Our Team

Stewart Ruffles

stewart.ruffles@thecleargroup.com
D: 0207 280 3479
M: 07572 104 029

Matthew Harvey

matthew.harvey@thecleargroup.com

D: 0207 280 3495

M: 07950 436 320

8. Supplier e-mail hacked

A manufacturing client received emails from a Chinese supplier & a Chinese employee, which appeared to be genuine. The emails requested that the payment owed be paid into a new bank account.

It is believed that the perpetrator(s) had hacked the email account of the Chinese employee to gain information about the business. This gave them access to the payment related communications between our client and their Chinese supplier.

The perpetrator(s) then carefully chose their moment to email our client requesting payments be made into "new" accounts. In total a payment of $23,000 (£17,800) was made and discovered on the same day. The claim was settled by Insurers (AIG).

9. Fraudulent change of bank details in genuine email

A supply and distribution client had genuine email communication with a supplier, but embedded within the email chain was a fraudulent notification regarding a change of bank details. Payment of approximately £115,000 was made to the 'new' bank details which were subsequently discovered to be false. This client did not have crime insurance in place.

10. RSA client loss

RSA's hotel client received a conference booking, costing £6,775.20, from a customer purporting to be from Dubai. The hotel received a payment for £67,752.00, which showed on the bank statement with a specific reference. The customer quickly followed this with a request for refund for the difference. The customer was very persistent and so, a few days later, the hotel's Financial Controller raised a payment request for the refund of £60,976.80 to be made.

The payment request was processed by the central finance team following the standard two-person approval. The next day, hotel staff identified that the £67,752.00 had been debited back to the bank account with a reference of "Unpaid Cheque" indicating that the cheque had bounced. It was subsequently discovered that the cheque was paid into a branch of HBSC in the UK.

Fortunately, there was insufficient cash in the bank account to enable the refund to be processed and as a result the refund failed, frustrating the fraud attempt. The incident was subsequently reported to the police by the Hotel Operations Manager.

Get in touch

We would recommend that businesses consider arranging crime insurance. For a quote and further guidance, contact one of our team members and they will be happy to help.