# Crime – Employee and Supplier Collusion Fraud

Collusion between trusted employees and suppliers can be difficult to detect, allowing fraud to continue unchecked until significant losses occur.

This Loss Prevention Standard highlights the key areas of risk to help support organisations.

Version: 1.1
Date: 5th November 2026

Aviva: Public

# Crime – Employee and Supplier Collusion Fraud

## Introduction



Organisations often recognise the threat posed by rogue employees and dishonest suppliers. However, some of the largest and most challenging fraud losses occur when trusted individuals from both sides of a business relationship work together to deceive the organisation. The transactions often appear legitimate, allowing these schemes to remain undetected for months or even years. Losses accumulate and create significant financial, operational and reputational consequences for the organisation.

Supplier collusion fraud can occur across any industry and in any size and type of organisation where employees have authority to influence purchasing decisions. It is rarely dramatic and doesn't typically begin with a large theft or a sophisticated cyber-attack. Instead, it often starts with a trusted employee, a long-standing supplier relationship and a small compromise of integrity. A procurement manager may accept a gift. A supplier may offer a favour. An invoice is approved without sufficient scrutiny. A contract is awarded without genuine competition. Over time, these small compromises become normalised and significant losses accumulate.

Because some goods may still be delivered and some services may still be performed, there is no suspicion and the fraud can remain hidden for years. The organisation believes it is operating normally, while excessive costs, inflated invoices or fraudulent payments quietly erode profitability.

## Understanding How Supplier Collusion Occurs

At its core, supplier collusion involves an employee abusing their position to benefit an external party, while receiving a personal benefit in return. This can take many forms and commonly involves:

- Direct financial gains through cash payments or kickbacks.
- A share of the profits when overcharging the organisation.
- Gifts, hospitality, holidays or personal services.
- Family favours or promises of future employment.

The result is often that the organisation ends up paying for goods or services that are only partly or never delivered, or paying a higher rate, with the colluding parties splitting the overpayment.

The supplier benefits by securing contracts, generating additional revenue or avoiding scrutiny. The employee benefits personally, whilst the employer ultimately bears the cost.

Unlike traditional theft, where money is simply stolen, collusion frequently disguises itself as legitimate business activity:

- Invoices appear genuine.
- Purchase orders exist.
- Suppliers are approved.
- Payments follow established processes.

Everything looks normal on the surface.

## Examples of Losses

These show how trusted employees and suppliers have exploited weak oversight, manipulated procurement processes and concealed inappropriate payments, resulting in substantial financial and reputational harm. The examples below illustrate some of the most common schemes and how they can develop.

### The Slow-Burning Fraud

Imagine a facilities manager responsible for overseeing maintenance contractors across a large manufacturing site. The organisation has used the same contractor for several years; the relationship is trusted and the supplier understands the business well. The contractor begins adding a small number of additional labour hours to monthly invoices.

The facilities manager notices but chooses not to question them. Months later, further charges are added, for example:

- Unnecessary call-out fees appear.
- Additional materials are billed but never supplied.
- Minor repair work is exaggerated.

In return, the facilities manager receives regular cash payments from the supplier. Individually, none of the invoices appear unusual. Collectively, they generate hundreds of thousands of pounds of excessive cost.

The fraud continues because the individual responsible for verifying the work is the same individual benefiting from the scheme. By the time concerns emerge through an audit or whistleblowing report, the losses may have accumulated over several years.

**Case Study - Long-Term Bribery and Inflated Contract Costs.** In May 2025, two former senior employees of large UK organisations were jailed after accepting more than £2 million in bribes from contractors in return for commercial contracts. Investigators found that payments and benefits were concealed through false invoices and company accounts. The scheme operated over several years and involved contractors receiving favourable treatment while the employees personally benefitted from the arrangements. [cps.gov.uk]

**Key Learning.** Long-running collusive frauds often succeed not because the fraudulent charges are sophisticated, but because trusted individuals are able to operate without effective challenge or oversight.

## The Hidden Cost of Contract Manipulation

Perhaps the most damaging form of supplier collusion is not the theft of money at all, but rather the manipulation of procurement decisions. Consider a procurement manager overseeing the award of a significant outsourcing contract:

- Several suppliers submit bids.
- One bidder has secretly agreed to pay a percentage of the contract value to the procurement manager responsible for the selection process.

The procurement manager influences scoring criteria, dismisses competing suppliers and recommends the preferred vendor. The contract is awarded and the organisation receives the service it expected. Outwardly, nothing appears to have gone wrong, yet the organisation may have paid considerably more than necessary, accepted lower-quality services or missed a better commercial opportunity.

**Case Study - Procurement Manipulation and Bribery.** In April 2025, three managers employed by a construction company were imprisoned after accepting over £600,000 in bribes from the owner of a demolition labour supplier. During the period in which the payments were made, the supplier benefited from contracts reportedly worth around £15 million. Prosecutors described the conduct as a serious breach of trust that distorted procurement decisions and competition. [cps.gov.uk]

**Key Learning.** Supplier collusion and procurement fraud have resulted in substantial losses across a wide range of sectors. Reported cases show how employees have manipulated procurement decisions, approved inflated costs, accepted bribes and created fictitious suppliers. Weak controls have often resulted in losses accumulating over a number of years before detection. The following examples illustrate some of the most common schemes and the financial damage they can cause.

## Telecommunications Contract Corruption

Employees with influence over procurement decisions may abuse their position by providing preferential treatment to a supplier in return for personal benefit. In this case, employees accepted cash, hospitality and other incentives in exchange for commercially sensitive information and favourable treatment during the contract award process. Although legitimate telecommunications services were supplied, procurement decisions were compromised and false, inflated and duplicate invoices were used to conceal the scheme and recover costs from the NHS. The arrangement continued for several years before being detected.

**Case Study - NHS Telecommunications Contract Corruption.** Four individuals, including two NHS managers and two supplier directors, were convicted following a long-running bribery and corruption scheme involving telecommunications contracts worth approximately £6 million across NHS Scotland. Investigators found that the NHS employees accepted cash, hospitality and other incentives worth more than £100,000 in return for providing commercially sensitive information and influencing the award of contracts. The investigation also identified false, inflated and duplicate invoices used to conceal the scheme and recover the costs from the NHS. The offenders received combined prison sentences totalling 29 years. [cfa.nhs.uk], [copfs.gov.uk]

**Key Learning.** Collusion between employees and suppliers can undermine even well-established procurement processes. Independent oversight, robust conflict-of-interest controls, supplier due diligence and detailed invoice scrutiny are essential to prevent long-running schemes from remaining undetected. [cfa.nhs.uk], [copfs.gov.uk]

### Supplier Relationships Influencing Purchasing Decisions

An employee develops undisclosed relationships with suppliers and receives financial incentives to purchase particular products or services. Although genuine goods are supplied, purchasing decisions are driven by personal gain rather than organisational need.

The resulting losses may arise from inflated prices, unnecessary purchases or the selection of less suitable suppliers.

**Case Study - Procurement fraud.** A former theatre manager at a Hospital Trust was convicted after accepting bribes from suppliers in return for influencing procurement decisions relating to medical equipment. A prosecution brought by the NHS Counter Fraud Authority found that the total value of the fraud, theft and bribery offences exceeded £600,000. Suppliers involved in the scheme were also convicted of bribery offences. [cfa.nhs.uk], [cfa.nhs.uk]

**Key learning.** Employees with influence over supplier selection and purchasing decisions pose a heightened collusion risk. Effective controls include supplier due diligence, segregation of duties, conflict-of-interest declarations, procurement audits and monitoring for unusual supplier concentration. According to the findings of the NHS Counter Fraud Authority, the fraud relied on improper supplier relationships and weaknesses in procurement oversight. [cfa.nhs.uk], [cfa.nhs.uk]

## Warning Signs Organisations Should Not Ignore

Very few collusive frauds begin without warning, but the signs can be missed, as they often appear insignificant in isolation. Whilst none of the indicators below prove wrongdoing, they may warrant further review:

- Employees who resist oversight or refuse to take annual leave.
- Unusually close relationships between employees and suppliers.
- Repeated use of a particular supplier despite competitive alternatives.
- Suppliers consistently winning contracts without challenge.
- Frequent retrospective approvals or urgent payment requests.
- Employees living beyond their apparent means or experiencing financial difficulties.

Long-serving and highly trusted employees can be particularly difficult to challenge because colleagues assume that integrity has already been proven. Changes in personal circumstances can also increase risk but can be difficult to spot. Often, when employee frauds are uncovered, investigations show that the motivation involves significant debt, gambling problems or other financial pressures.

Supplier behaviour may provide equally important clues like:

- Recently established businesses winning substantial contracts.
- Repeated requests to change bank account details.
- Excessive invoice amendments.
- A concentration of spend with a single supplier.

Several of these indicators appearing together could suggest an elevated risk and organisations should investigate rather than assume and accept that there is an innocent explanation.

## Building Effective Defences

The most effective fraud controls are those that make collusion difficult to establish, hard to conceal and easy to detect. While no control can completely eliminate the risk, a layered approach can significantly reduce the opportunity for employees and suppliers to work together to defraud the organisation. These include:

**Segregate Key Activities.** No individual should control the entire procurement and payment process, and independence should be integral to the following areas:

- Supplier onboarding.
- Purchase approval.
- Goods receipt.
- Invoice approval.
- Payment release should be performed by different people wherever practical.

Collusion often succeeds when a trusted employee can influence multiple stages of a transaction without independent challenge. Even where resources are limited, organisations should set thresholds and ensure that high-value transactions, new suppliers and changes to supplier details receive independent review.

**Strengthen Supplier Due Diligence.** Organisations should understand exactly who they are doing business with before entering into a commercial relationship. Due diligence should extend beyond financial stability and include:

- Verification of company registration and ownership.
- Identification of ultimate beneficial owners.
- Review of trading history and online presence.
- Checks for conflicts of interest involving employees, directors or family members.
- Screening for sanctions, regulatory actions or adverse media where appropriate.

Supplier declarations requiring disclosure of any employee relationships can also help identify potential conflicts before losses occur.

**Maintain Accurate Supplier Records.** Supplier master file controls are often an overlooked defence against collusive fraud. Organisations should regularly review supplier data for:

- Duplicate addresses, telephone numbers or email addresses.
- Multiple suppliers using the same bank account.
- Suppliers sharing details with employees.
- Dormant suppliers that suddenly become active.
- Unusual changes to bank account information.
- Suppliers receiving payments outside normal procurement processes.

Any changes to supplier bank details should always be independently verified using trusted contact information rather than details provided within an invoice or email.

**Use Data Analytics, AI and Transaction Monitoring.** Technology can identify patterns that are difficult to detect through manual review. Analytics and transaction monitoring around spending can help identify:

- Duplicate or near-duplicate invoices.
- Round-sum payments.
- Split invoices designed to avoid approval thresholds.
- Significant increases in spend with a particular supplier.
- Payments made outside normal business hours.
- Excessive supplier concentration within a department.
- Invoices submitted immediately below delegated authority limits.

Ensuring regular exception reporting allows management to focus reviews on higher-risk transactions rather than relying solely on periodic audits.

**Conduct Independent Supplier Reviews.** Periodic supplier audits can help verify that suppliers remain legitimate and continue to provide value for money. Reviews may include:

- Confirmation that goods or services were genuinely received.
- Benchmarking prices against alternative suppliers.
- Validation of contract terms and deliverables.
- Physical checks where goods are involved.
- Reconfirmation of ownership and beneficial control.

Independent reviews can be particularly valuable where a supplier has a long-standing relationship with the organisation, as familiarity can reduce levels of scrutiny over time.

## Creating a Culture That Challenges

Even the strongest controls can be circumvented when employees and suppliers work together. As a result, organisations should not rely solely on processes and technology. Employees at all levels should understand that procurement decisions, supplier relationships and payment activity are open to scrutiny and challenge.

Managers should encourage staff to ask questions when something appears unusual, such as:

- Why is the same supplier repeatedly awarded work without competition?
- Why does one employee appear to have an unusually close relationship with a supplier?
- Why are invoices regularly approved urgently or outside normal processes?
- Why are contract values increasing without a clear commercial rationale?
- Why does a supplier continue to be used despite poor performance or higher costs than competitors?
- Why are supplier bank details changing frequently?

Employees should understand that raising these questions is not an accusation of wrongdoing but a normal part of protecting the organisation and should not fear retaliation when reporting. Organisations should also maintain confidential reporting channels and actively promote their use. Employees are often the first to notice unusual behaviours, conflicts of interest or procurement irregularities. Encouraging concerns to be raised early and ensuring reports are investigated objectively can prevent relatively small issues from developing into significant financial losses.

Fraud awareness training should include practical examples of supplier collusion schemes and the warning signs that may indicate elevated risk, including:

- Employees who resist oversight, refuse to take annual leave or insist on handling supplier relationships personally.
- Suppliers and employees socialising excessively or having undisclosed personal relationships.
- Repeated contract awards to the same supplier despite alternative options.
- Supplier invoices that consistently fall just below delegated authority limits.

It is important that senior leaders set the tone. Where management behaviours visibly challenge supplier spending, question procurement decisions and demonstrate zero tolerance for conflicts of interest, employees are more likely to recognise that supplier relationships are subject to scrutiny and accountability.

## Key Takeaways

Supplier collusion fraud is one of the most difficult forms of employee dishonesty to detect because it exploits trust on both sides of a commercial relationship.
The fraud often hides behind apparently legitimate invoices, contracts and business transactions, allowing losses to accumulate over long periods before discovery.

Any organisation that purchases goods or services from external suppliers is potentially exposed, regardless of size or sector.

Strong procurement governance, effective segregation of duties, supplier due diligence and a culture that encourages challenge remain the most effective safeguards.

## Contact Information

### Canada

Please visit Aviva Risk Management Solutions | Aviva Canada or email us at arms.canada@aviva.com

### Ireland

Please visit Insurance Risk Management | Business Risk Management Insurance - Aviva Ireland or Email us at armsireland@aviva.com

### United Kingdom

Please visit Aviva Risk Management Solutions or email us at riskadvice@aviva.com. To speak to one of our advisors, call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

# Specialist Partner Services

Aviva have created a network of Specialist Partners to complement our in-house capabilities and to enable our policyholders to benefit from a wide range of risk management solutions at preferential rates and terms. Together, we provide solutions to help with the significant challenges of modern-day risk management.

**Note:** These partner relationships are wholly for the benefit of our policyholders with no income to Aviva.

The following Specialist Partners provide products or services in relation to risk guidance provided, discussed or referenced in this Loss Prevention Standard.

### Canada

For more information please visit: Our Specialist Partner Network | Aviva Canada

### Ireland

For more information please visit: Insurance Risk Management | Business Risk Management Insurance - Aviva Ireland

### United Kingdom

For more information please visit: Aviva Risk Management Solutions – Specialist Partners

# Standards, Sources and Useful Links

### Canada

- Canadian Anti-Fraud Centre
- National Cybercrime and Fraud Reporting System

### Ireland

- National Cyber Security Centre

### United Kingdom

- Credit Industry Fraud Avoidance System (CIFAS)
- National Fraud Intelligence Bureau
- UK Finance Fraud Report 2026
- FraudTrack 2025 | UK Fraud News - BDO
- CIFAS Guide - Prevent Fraud for Organisations | Private, Public and Charity

### Other

- Internet Crime Complaint Center

# Additional Information

## Loss Prevention Standards

These documents set out best practice recommendations to help reduce the likelihood and impact of losses.

Relevant Aviva Loss Prevention Standards include:

- **Crime – Employee Fraud, Theft and Dishonesty**
- **Crime – Mergers & Acquisitions Exposures**
- **Social Engineering Fundamentals**

Please visit Loss Prevention Standards to view the full library.

## Aviva Risks Training Solutions (United Kingdom Only)

Aviva Risk Training Solutions, delivered through our Specialist Partner, SafetyCulture, provide free, bite-sized learning modules exclusively for Aviva policyholders.

Relevant courses include:

- **Social Engineering**

Please visit Aviva Risk Training Solutions for further guidance.

**Please Note**

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. By extension, any links to third-party websites do not constitute marketing by Aviva and are included solely for the reader's information and educational purposes. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise, and Aviva recommend that you obtain specific advice relevant to the circumstances.

5th November 2026

Version 1.1

ARMSGI5282026

Aviva Insurance Limited, Registered in Scotland Number SC002116. Registered Office: Pitheavlis, Perth PH2 0NH.
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.