

Crime – Mergers and Acquisitions Exposures

Fraud risk management needs to be a key consideration during the merger and acquisitions process.

This Loss Prevention Standard highlights the key risk management guidance to help support organisations.

Crime – Mergers and Acquisitions Exposures

Introduction

Mergers and acquisitions (M&A) can be exciting opportunities for growth, but they also create a perfect environment for fraud.

Large amounts of money are changing hands, sensitive information is being shared, and a small group of people are often working to tight deadlines under strict confidentiality.

Criminals understand the pressures surrounding a transaction and look to exploit them for their own gain. They know employees expect unusual requests, they know confidentiality limits open discussion, and they know senior executives are heavily involved, making them obvious targets for social engineering. When urgency, secrecy and authority are combined, normal verification processes can be overlooked and even experienced employees can find themselves making decisions they would normally pause to question.

From a crime risk perspective, M&A activity should be viewed as a period of heightened vulnerability, where controls need to be strengthened rather than relaxed.



Key Considerations

M&A transactions often involve multiple parties communicating across various platforms. Criminals may compromise email accounts or exploit messaging platforms to infiltrate communication chains, enabling them to redirect payments or alter bank account details and payment instructions. Because the transaction itself is unusual, fraudulent requests can be difficult to distinguish from legitimate activity.

Warning signs include:

- Last-minute changes to bank account details.
- Requests involving unusual urgency.
- Instructions that discourage independent verification.
- Payment requests to unfamiliar jurisdictions.
- Changes communicated through alternative messaging channels, such as WhatsApp or text messages.

During times of M&A activity, it can also be easy to overlook the insider risk. It is important to consider the role of employees throughout the process and whether disgruntled employees may pose a threat, as acquisitions can create uncertainty around roles, responsibilities and future employment. In any organisational change, staff departures and system integrations can all weaken established controls, and in some cases, employees may exploit temporary control weaknesses.

In other cases, they may themselves become targets for criminals seeking information, access credentials or other assistance.

The increased internal activity when an organisation is readying itself for an acquisition frequently brings increased scrutiny of financial records, controls and processes. As a result, frauds that previously went undetected are sometimes uncovered during due diligence or post-acquisition reviews. Organisations should recognise that a transaction may expose historic control failures or issues that were not previously known.

Set out below, are some precautionary measures to consider during the lifecycle of the transaction to help manage the potential risks.

Before the Transaction

The period before a transaction completes provides the best opportunity to review and reduce fraud exposure. Decisions made at this stage will often determine how effectively the organisation can identify, prevent and respond to fraud risks throughout the transaction. Alongside traditional financial and legal due diligence, organisations should ensure that governance, payment controls, communication protocols and employee awareness arrangements are robust enough to support what is often a high-pressure and fast-moving process.

Some core considerations are set out below:

Governance and Payment Controls

- Identify individuals with authority to create, approve and release payments.
- Review segregation of duties to ensure no individual has excessive control over payment processes.
- Establish enhanced approval requirements for transaction-related payments.
- Confirm escalation procedures for unusual or high-risk requests.

Verification Procedures

- Agree how payment instructions and banking details will be independently verified.
- Ensure all parties understand that confidentiality does not remove the requirement for verification.
- Establish trusted contact information for advisers, lawyers and transaction counterparties.
- Require all changes to payment instructions to be validated through independent channels.

Security of Communications

- Review email security and multi-factor authentication arrangements.
- Identify approved communication channels for deal-related activity.
- Restrict the use of informal messaging platforms for financial instructions wherever possible.

Employee Awareness

- Ensure individuals involved in the transaction understand the heightened fraud risks.
- Provide guidance on deepfake, impersonation and payment diversion threats.
- Reinforce expectations around challenge, escalation and verification.
- Promote a culture where employees are encouraged to question unusual requests.

During the Transaction

Once a transaction is underway, maintaining disciplined execution becomes critical. The focus should be on ensuring that established controls continue to operate effectively despite increased workloads, accelerated decision-making and heightened levels of confidentiality. This is not typically the time to introduce new processes, but rather to ensure that existing controls are consistently applied, particularly where significant financial transactions or changes to payment instructions are involved. Some core control measures are set out below:

Payment Instruction Validation

- Independently verify all payment instructions before funds are released.
- Apply enhanced scrutiny to any changes to beneficiary details.
- Validate requests using trusted contact information rather than details contained within the instruction.
- Treat last-minute changes as high-risk events requiring management review.

Protection Against Social Engineering

- Be alert to requests involving urgency, secrecy or pressure.
- Challenge any attempt to circumvent established controls.
- Verify instructions appearing to originate from senior executives, law firms or advisers.
- Communicate any increased or emerging fraud risks to employees throughout the transaction period.

Enhanced Approval and Oversight

- Maintain dual authorisation requirements for material payments.
- Ensure appropriate management oversight of transaction-related activity.
- Monitor for unusual payment patterns or exceptions.
- Avoid introducing temporary control workarounds to accelerate completion.

Speak-Up Culture

- Encourage employees to raise concerns where requests appear unusual.
- Support challenge regardless of seniority or perceived authority.
- Clearly communicate escalation routes.
- Reinforce that delaying a payment for verification purposes is preferable to releasing funds in error.

After Completion

Completion should not be viewed as the end of the risk management process. The integration phase often involves significant operational change, including system migrations, revised reporting structures, changes in responsibilities and the adoption of new processes. Ensuring that controls remain effective and consistent across the combined organisation is essential to reducing the risk of fraud, control failures and operational disruption as the business transitions into its new structure. Effective integration is key to ensuring that these risks are identified and addressed.

Core elements of this process are set out below:

Control Environment Integration

- Apply the organisation's financial control framework to the acquired entity as soon as practical.
- Align approval authorities and payment controls.
- Standardise reconciliation and exception reporting processes.
- Ensure governance arrangements are clearly understood.

Identity and Access Management

- Review user access rights across financial and operational systems.
- Remove unnecessary or dormant accounts.
- Review privileged access and administrator permissions.
- Align access controls with revised roles and responsibilities.

Monitoring and Oversight

- Increase monitoring of high-risk financial transactions during integration.
- Review supplier onboarding and bank account amendment activity.
- Monitor for unusual behaviour, policy breaches or control circumvention.
- Escalate anomalies promptly for investigation.

Fraud Risk Validation

- Reassess assumptions made during due diligence.
- Conduct targeted reviews of payments, suppliers and reconciliations.
- Investigate any historic discrepancies identified during integration.
- Validate that acquired operations are operating within the organisation's risk management framework.

Key Takeaway

Fraud risk management should form a key part of the due diligence process, alongside financial, legal and operational reviews. Assessing the target organisation's control environment, governance framework, payment processes and fraud prevention measures can help identify vulnerabilities, historical issues and areas requiring remediation before completion.

By incorporating fraud risk considerations at an early stage, organisations are better positioned to make informed decisions, prioritise integration activities and establish a strong control environment from day one.

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.

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](#)
- [National Fraud Intelligence Bureau](#)

Other

- [Internet Crime Complaint Center](#)

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:

- **Payee Verification Policy**
- **Social Engineering fundamentals**
- **Social Engineering Fraud – Sim-swap and Ghost-pairing**
- **Cyber – Mergers & Acquisitions Exposures**

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:

- **Cyber Fundamentals**
- **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.

24th September 2026

Version 1.0

ARMSGI5132026

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.