



# Risks of operating in a remote environment

---

**Nikki Bowker, Partner**  
**Litigation and Dispute Resolution**

11 October 2022

# Fraud in a remote environment

- Pre-Covid corporate fraud was widespread
- Covid forced organisations to transition to remote working/operation
- Transition expedited and often unplanned
- Workarounds put in place to circumvent practical/logistical difficulties

# Fraud: whistlestop tour

- Criminal and civil jurisdictions
- Fraud Act 2006:
  - Fraud by false representation (section 2)
  - Fraud by failing to disclose information (section 3)
  - Fraud by abuse of position (section 4)
- Theft Act 1968:
  - False accounting (section 17)
  - False statements by company directors (section 19)
- Common Law:
  - Deceit, conspiracy, breach of fiduciary duty, breach of trust, dishonest assistance, conversion, restitution

# Fraud statistics

- ONS: Nature of fraud and computer misuse in England and Wales (YE March 2022)
  - Fraud offences increased by 25% compared with YE 2021
  - Cyber fraud incidents increased to 61% from 53%
- PwC's Global Economic Crime and Fraud Survey 2022
  - 46% of surveyed organisations reported experiencing some form of fraud or other economic crime within the last 24 months
  - Across organisations of all sizes, cybercrime poses the biggest threat, followed by customer fraud and asset misappropriation
  - Nearly 70% of organisations experiencing fraud reported that the most disruptive incident came via an external attack or collusion between external and internal sources
  - 1 in 8 organisations experienced new incidents of supply chain fraud as a result of disruption caused by Covid

# Why should I worry?

- Corporate fraud is widespread, costly and ever evolving
- Identification and recovery of losses is more expensive and difficult than prevention
- Financial – actual loss, opportunity loss (diverted attention and management time)
- Regulatory – heightened scrutiny from RSH, possible downgrade, access to banking facilities
- PR implications – brand damage, consumer distrust, investor uncertainty

# The Covid effect

- Home working
- Face-to-face interaction reduced
- Increase in expectation that fraud will not be detected
- Greater reliance on emails – increased exposure to interception related frauds
- Fast tracking of established procedures – e.g. payment authority (electronic signatures)
- Staff turnover
- Empty office space

# Types of fraud we see in Registered Providers

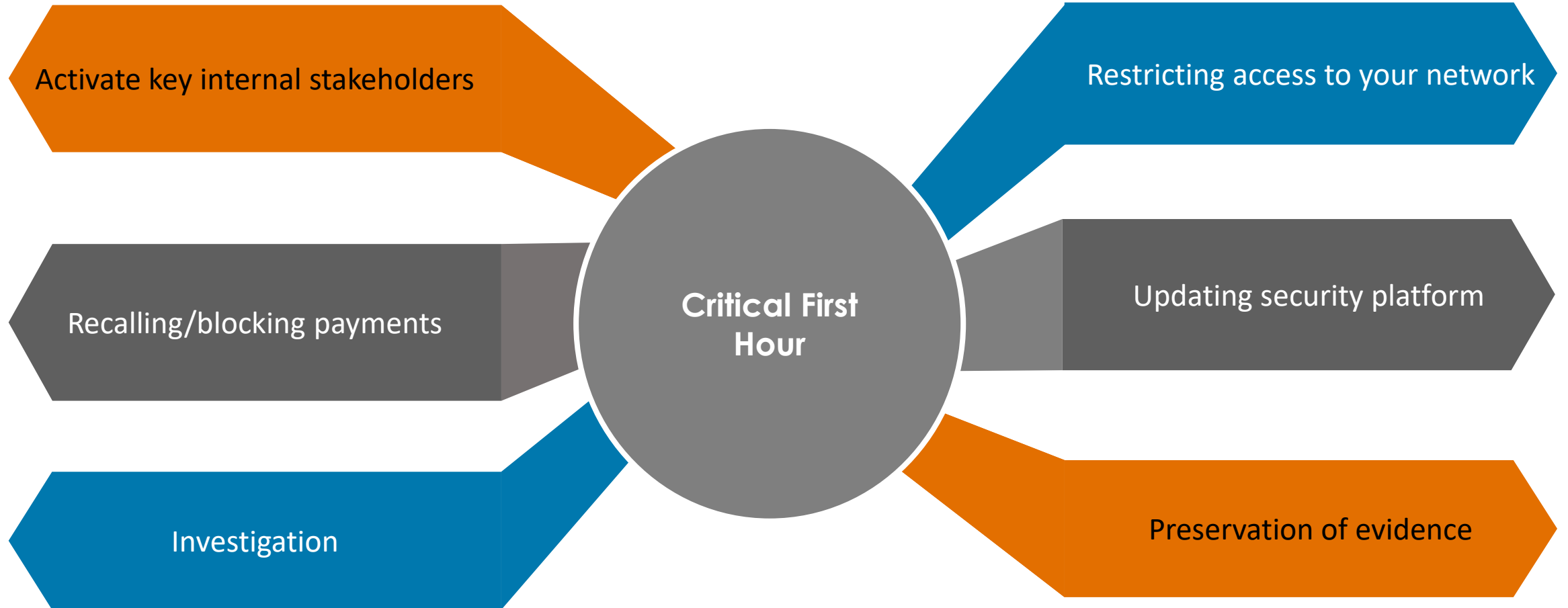
- Procurement fraud:
  - Securing appointment of preferred supplier (tender manipulation);
  - Agreeing inflated payments/rates; and
  - Agreeing additional services which are never provided.
- Email intercept fraud
- Third party impersonating organisation to trap customers and investors
- Often some form of relationship between employee and third party
- Internal fraudster can be at any level
- Fraud is routinely not discovered for several years

# Possible fraud indicators

- Supplier/provider with no sector or industry experience
- Supplier/provider whose turnover is largely reliant on one organisation
- Round sum invoices and invoices with no detail of work/services
- Underperforming contracts/relationships
- Onboarding process fast-tracked







Activate key internal stakeholders

Restricting access to your network

Recalling/blocking payments

Updating security platform

Critical First Hour

Investigation

Preservation of evidence

# Investigating fraud

- Identify the allegations:
  - What is being alleged?
  - What are the concerns?
  - Are they capable of investigation?
  - Be specific
- Conducting the investigation
  - Control the investigation – defined parameters
  - Lead investigator
  - Document retention, capture and review – may need specialist IT support
- Discretion – email/networking searches, remote access to work devices, personal emails, slack space

# Investigating the fraudsters

- Use public information:
  - Companies House
  - Experian
  - Social media (including for their family)
  - Internet search
  - Newspapers – local and national
  - Proximity of homes
  - Bankruptcy
  - Land Registry

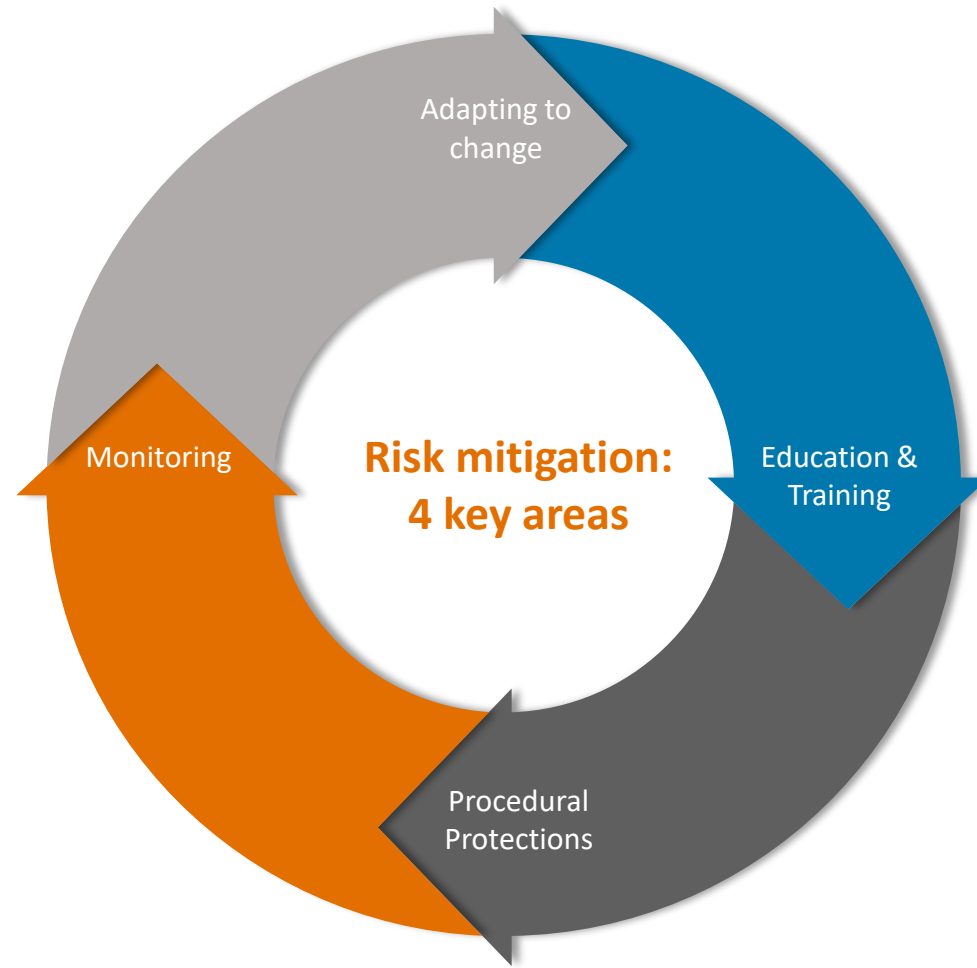
# The evidence has been gathered: what next?

- Don't delay
- Consider any emerging lines of investigation
- Challenge the witnesses and possible perpetrators if appropriate
- Access bank account data – Bankers Book Evidence Act 1879
- Third party disclosure
- Freezing injunction
- Search and seizure orders

# Recovery

- Insurers – beware condition precedents and duty to mitigate loss
- Banks
- Accountants/Auditors
- Fraudsters
- Dishonest assistance (can catch internal fraudsters with this)

# Risk mitigation



# Education & Training

- Awareness of specific industry risks
- Top down approach
- Ethics policies/Codes of Conduct
- Appropriate staff training
  - On-boarding
  - Annual training
  - Red Flag awareness
- Perception of strict practice



# Procedural Protections

- Due diligence for employees and contractors
- Bank mandates
- Transactional security
- Segregation of accounting duties
- Limited on authority
- Changes to standing instructions
- Oversight and cross-checking

# Monitoring

- Continuous and periodic
- Employee monitoring
- Financial monitoring
- Team/project audits
- Red flag awareness
- Whistleblowing policy
- Escalation mechanism

# Adapting to Change

- Annual review of fraud risk profile:
  - Industry
  - Technological changes
  - Internal changes
  - Board Report
- Updated phishing and penetration testing
- Consider how these changes affect your preparedness – don't stand still!

# Fraud risks during economic instability

- Assess reliance on third parties – any that may go bust and would you have time for the normal vetting process before onboarding new parties
- Economic instability draws management focus and attention which could reduce oversight elsewhere
- Cost of living crisis could drive fraud perpetrated by/in collusion with internal actors

## Case examples



- Toy Co – email intercept fraud – loss of £200,000
- RP – Fake £50m bond issue through use of copy-cat website
- RP – procurement fraud on telecoms contract – employee receiving kick-backs

# Q&A