

Fraud...

Nothing to see here



tenet

Introducing a thought-provoking whitepaper focused on the affordable housing sector co-authored by Tenet Law and Newid Consulting. In this report we challenge the perception that the risk and impact of fraud is often understated among Registered Providers of affordable housing. We follow up as we explore the proactive measures that can and should be taken to combat fraud ensuring both financial and social returns are maximised.



Introduction

When it comes to fraud in the context of affordable housing, what immediately springs to mind? This question has been itching at the minds of Arun Chauhan from Tenet Law and Paul Roberts from Newid Consulting for quite some time.

Cybercrime, supplier payments, expenses, and tenancy fraud risks often are seen as the obvious important areas to consider. However, as you'll soon discover in this Whitepaper, there are more aspects to consider, in some cases, the tackling of these issues is not as effective as it could be and deeper impact and benefit from considering fraud in a new light.

Preventing and mitigating fraud risk shouldn't be viewed as extra work, but rather an opportunity to cultivate a better culture and improve our processes and above all, do what is right. For housing associations, fraud is not just about loss of money. The waste and misuse of that money takes away from the very purpose that drives the sector – providing affordable housing.

If it is the case that fraud isn't talked about or understood sufficiently for risk registers or to inform the wider cultural impact and, if we do nothing, could it be the next sleeping giant that catches us out given the political landscape now progressing the failure to prevent fraud offence?

Contents

- 3 Authors
- 4 Setting The Scene
- 5 Why Affordable Housing?
- 6 Fraud Types
- 7 Examples of Fraud
- 8 Culture and Fraud
- 9 Impact
- 10 Prevention
- 11 Wider Issues for ARC
- 12 Benefits
- 13 Best Practice Guide
- 14 The State of Play
- 15 Culture, Tools and Collaboration



Abstract

This Whitepaper seeks to inform the debate about the types of fraud which may exist. Some may be more obvious than others against the backdrop of recognised causes, ranging from the cost-of-living crisis, gaps in controls, system and organisation change as well as a raft of challenging sectorial priorities which inevitably require immediate and sustained attention. In addition, we suggest practical solutions that can lead to marginal improvements for some and perhaps more significant improvements for others.

This Whitepaper aims to spark the interest of all those engaged in defending their organisations, customers, and themselves against fraud. We also hope that it will initiate a dialogue with the sector's regulator to influence future editions of the Sector Risk Profile report. By doing so, we aim to contribute towards the protection of affordable housing assets.

Fraud prevention is about human firewalls and human controls – people can be your eyes and ears and it's not embedded enough.



Arun is an accomplished lawyer specialising in disputes and compliance investigations, bringing successful litigation claims to recover loss from financial fraud having acted for housing associations for over 10 years in these types of cases. Founder of disruptive law firm Tenet, the only niche law firm in its field outside of London and winner of Boutique Law Firm 2022 at the prestigious Legal Business Awards. Arun is a regular fraud expert for the BBC, speaks at National Housing Federation and other affordable housing events and has been quoted in The Times, The Guardian and The Telegraph. He is Trustee Director for the Fraud Advisory Panel and provided evidence to a House of Lords Committee about the impact of digital fraud and effectiveness of the 2006 Fraud Act. Arun is experienced in working closely with clients across the affordable housing sector on training, improving policies, conducting investigations, and recovering any losses suffered.

Arun Chauhan

Email: arun.chauhan@tenetlaw.co.uk



Paul has over 30 years of expertise in finance, risk, governance, leadership, ICT and strategy, across business sectors, including over a decade of housing sector experience in an executive role at the Guinness Partnership. Paul currently acts as an independent consultant working with housing associations and charities to develop their approach to Environmental, Social, and Corporate Governance (ESG), housing strategy, repairs and maintenance, social investment and internal controls. He has served as Chair at Regenda Group and is currently a Non-executive Director with Gloucester City Homes, Auxesia Homes and the new Chair of the Audit & Risk Committee at Rochdale Boroughwide Housing.

Paul Roberts

par.newid@outlook.com

Setting The Scene

Much of the sector remains either unconscious to the wider risks or consciously not dealing with them as *"it's not something that affects us"*. When Registered Provider (RPs) annually submit nil report after nil report with what appears to be little to no feedback from the Regulator of Social Housing (the **"Regulator"**), a false perception of immunity becomes somewhat inevitable. If the Regulator considers there are no significant issues of concern, prioritisation of fraud in RPs organisation eco-system is diminished in part because the Regulator is not driving forward the message to be more pro-active.

Is there really *'nothing to see here'*, or are **growing** risks hiding in plain sight?

As digital innovation continues to grow, we have rightly recognised that the risk of cybercrime has become more prevalent. Alongside this, there are other areas that are also at risk, such as payroll, accounts payable, procurement (onboarding and monitoring of suppliers), and tenancy fraud. The critical question at hand is whether we are diligently implementing measures to identify risk, prevent, investigate, and respond to these incidents?

Meanwhile, what about the susceptibility to fraud elsewhere in our organisations as well as for our key stakeholders, customers and colleagues?

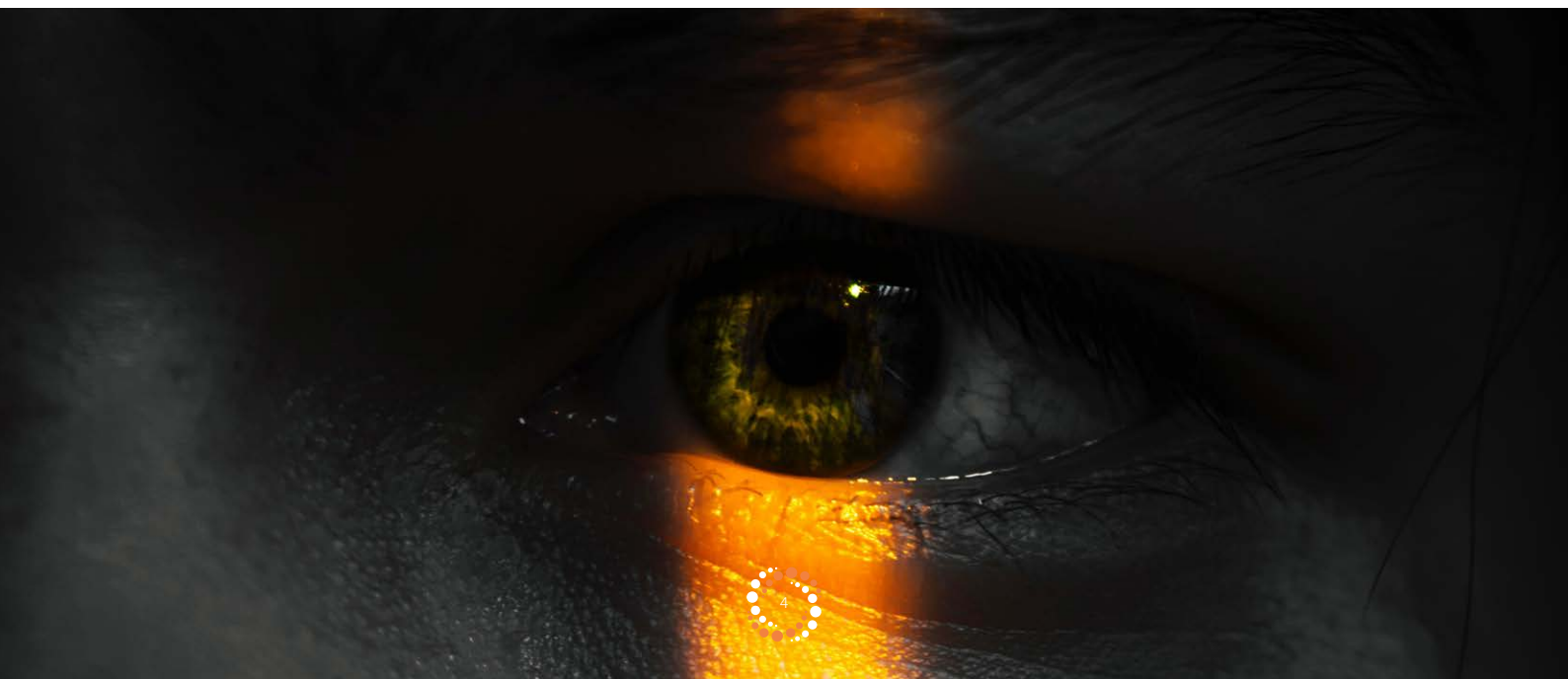
Are our Boards, executives, managers, and operational staff on the front line well-informed about the vulnerability to fraud in our sector? The Regulator includes fraud briefly in the Sector Risk Profile referring to the usual areas we have highlighted above.

We must magnify the situation on the ground and explain the lesser-known aspects of fraud not only to senior leadership, but to the wider employees working tirelessly in the sector who might not know what fraud actually *'feels like, smells like or looks like'* in everyday business operations. This is especially important because fraud tends to thrive in certain conditions, as we will discuss later.

In today's business landscape, the threat of fraud from external and internal sources looms over organisations across every sector so much so that fraud and cybercrime account for 41% of all crime in the UK. We must therefore ask ourselves, why is it affordable housing has a trend of nil returns? What makes affordable housing immune to the impact all other sectors are alive to? It is only when we understand this can we consider the impact, devise and develop preventative measures, and pursue the benefits of a proactive approach against fraud be that fraud impacting our organisations and affecting our people.

Is enough being done or is fraud risk and cost being normalised?

Are we turning a blind eye because we have tunnel vision in part because of the other big and critical issues we face, from concrete, cladding to consumer regulation?



Why Affordable Housing?

The affordable housing sector has many risks to consider, representing an ecosystem that makes an organisation exposed to a variety of frauds which are ever evolving. The mounting pressure on the Regulator and RPs is widely acknowledged, and there is a growing concern that amidst this vulnerability, fraud – including against tenants and staff – could be another source of reputational as well as financial damage for the sector.

Generally speaking, the **average organisation loses 3-10% of total revenue** to fraud each year. Is this simply the “*cost of doing business*” for RPs and therefore are they turning a blind eye to fraudulent activity that has become normalised and slips under the radar? Or is it, like other issues that have arisen over this century for the sector, simply been sitting hidden in plain sight to a greater or lesser extent, unable to be detected due to distraction with more pressing issues, a lack of investment or understanding, or ongoing relentless internally and externally led change.

In a sector where RPs typically hold significant value of assets, have a large number of employees, numerous suppliers of differing types, are increasingly dependent on IT, hold valuable data and make substantial amounts of financial transactions a year, this offers access to valuable assets at lower cost (i.e. properties), it is no wonder that this is one of the most diverse and vulnerable sectors exposed to fraud.

Consistent and sustained communication about this very point as to the exposure to fraud risk, stronger thought leadership, greater collaboration and meaningful education is needed – forming an ultimate outcome of supportive co-regulation and cultural ownership that proactively responds to this ever-evolving and fast moving danger.



Fraud Types

What does fraud look like in affordable housing?

Common types of fraud affecting housing associations fall into two categories: Corporate Fraud and Tenancy Fraud. While we often hear about the most common types of fraud, it's important to be aware of the less talked-about ones. These less-known frauds might not be well understood, and it's crucial to examine how they are being identified and dealt with. Sometimes, fraud in affordable housing can arise from unexpected sources.

Corporate fraud

- Bribery and collusion
- Cybercrime
- Supplier fraud
- Mandate fraud
- Payroll fraud
- Finance function fraud
- Recruitment fraud

Tenancy Fraud

- Application fraud
- Right-to-buy/acquire fraud
- Key-selling fraud
- Subletting (and subletting of part) fraud
- Succession fraud



Defining Fraud

There is no doubt that the COVID pandemic led to an increase in fraud; the pressure to make ends meet which has now extended to the cost of living crisis has led to more people finding opportunities to commit fraud, home working idrove and continues to cause a change in behaviours. The volume of emails and pace expected on communications of staff has also contributed to an increase in cybercrime, mistakes and concealment.

The truth is that whilst most organisations are aware of the need for fraud prevention education, many still have the mindset of *"it will never happen to us"*. Much of the root cause of this comes from two areas. Firstly, that there is not a clear and uniform understanding of what *"fraud"* is amongst employees. Fraud is not black and white, dishonesty comes in many shades and to some, that leaves their conduct open to interpretation. Certain conduct may be seen as fraud, for others it is sharp practice. It may well also be areas previously not considered as fraudulent, but actually do meet the definition when debated e.g. former tenant arrears, detrimental conflicts of interest, data leaks, money laundering risk through cash payment of arrears to name but a few.

Secondly, there is a misunderstanding around trust; dependent on a range of circumstances, good people can do bad things. Whilst trust in a workplace is essential, it should not be at the expense of being aware of how fraud can be perpetrated against your own organisation. Trust is not a control in itself, guardrails are still required.

We need to think about the fringes of fraud and explore those risks just as diligently to make the links across our business operations.

Examples of FRAUD

- Paying rent arrears with cash in carrier bags
- Airbnb/Zoopla short term tenancy letting fraud applicable to rented as well as shared ownership homes
- Money laundering through RTB or RTA schemes
- Sharing tenant's data with organised crime in return for a financial reward.
- Stolen equipment, from low value office items to higher value planned maintenance stock
- On-the-side contractor work, use of company vehicles and equipment
- Long-standing employees with multiple supplier links
- Employees varying the procurement monitoring, payment or onboarding processes to the preference of certain suppliers.
- Preferring a supplier in exchange for financial or non-financial benefit.
- Diverting money from your organisation for fictional suppliers orchestrated by a rogue employee.

When considering just these handful of fraud examples impacting the sector, it is our view that in the current climate where the Government has driven change in the laws on corporate criminal liability around economic crime, most recently having created offences around failure to prevent fraud, the sector must consider refreshing its language when it comes to fraud and wider financial crime. The sector need to broaden definitions and appreciate why this is a key area of focus for many sectors right now.

Whilst corporate maturity i.e. a desire to prevent fraud and financial crime is a key driver, we firmly believe that leading from the front to prevent fraud will lead to positive financial and cultural returns from proactively preventing fraud.

Culture and Fraud

Fraud is not so clear-cut; it is about interpretation. We as a sector have not consistently steered our people to understand these dynamics and why there are various risks not only to an RP, but also to its people. One area not talked about enough here is culture. Fraud is a vicious crime not just impacting RPs, but also its' people as consumers at risk in their day to day lives. Helping employees understand the threat of fraud to them (and their families) brings an embracing approach of protection of your people which can pay back significantly as your 'human firewall' protects your organisation. They are still your best eyes and ears although A.I. should be an important tool in the near future.

Historically, the sector has perhaps fallen foul of a lack of consistent and sustained anti-fraud communication, along with an undesirable workplace culture which together have fostered an environment which makes fraud all the more likely in a given organisation – where people are motivated to do the 'right thing' for themselves, rather than the actual 'right thing'.

The traditional fraud triangle emphasises that pressure can lead to an act of fraud. The employee rationalises their choice in that given moment in their life. Pressure of home debt, performance metrics at work or wider pressures can lead to good people making an unwise choice one would not expect of them. They can take up the opportunity that might present itself in the workplace to better their position when they were not entitled to it. Their situational circumstances only discovered after news of an employee fraud emerges often are surprising and invariably lead to the shock that good people can do bad things.

When it comes to the motives of external individuals and entities to commit fraud, whilst financial gain tends to be thought of a prominent factor, we forget that it is what is driving the need for that financial gain which is the crucial factor. When we do not have a cultural mindset and approach at work of openness that we can identify where certain employees or suppliers might be subject to increased pressures, we then see that inadequate internal controls and oversight, lack of awareness, inadequate policies and procedures can make it easier for fraud to occur unnoticed or unchallenged.

Culture plays a pivotal role regardless of the source of fraud, as culture that tolerates or even encourages any unethical behaviour can result in fraud being normalised. Fear of retaliation, ignorance, and denial can deter people from reporting fraud, while the complexity of fraudulent activities may go unnoticed due to a lack of knowledge or resources. This fear can discourage whistleblowing and encourage a culture of silence.

If fraud has been occurring within a company for a long time without consequences, it can become ingrained in the culture, making it harder to mitigate.

A focus on trust and credibility may lead to RPs 'turning a blind eye' denying any existence of fraud. The desire to protect the organisations reputation is essential for building long term sustainability and positive relationships with stakeholders. With the significant lack of data sharing across sectors, it can be easy to remain unaware of fraud risks to maintain a favourable relationship with the Regulator and give the impression that an organisation is compliant and acting ethically.

The Silence is Deafening

Nil return after nil return essentially saying there is "nothing to see here" makes that silence deafening. Addressing the issue is crucial, regardless of the motivation behind the silence or the low level of proactiveness in spotting potential risks on the fringes of fraud.

As a sector, we must establish a uniform approach to embedding an ethical culture, implementing strong internal controls that align with how each organisation delivers their work, and promote a zero-tolerance policy for fraud.

Whilst we know that regulatory oversight and legal consequences can also act as deterrents, encouraging businesses to take a proactive stance now more than ever seem to be the most important driver for change.

This is where more focused fraud awareness is key. The starting point is understanding what it is and how far ranging its impact is. Only then training and development can contribute to proactive, anti-fraud processes, but also raise professional standards through constructive curiosity and improved skills.

In so doing these complement corporate culture which is focused on collaborative effort towards organisational purpose, the use of resources efficiently and effectively to drive service delivery to customers and tenants, to seek continuous improvement and provide stable and rewarding jobs.

In other words, each sector ought to strive for their employees knowing why fraud prevention is so vital when it comes to protecting each other and your organisation.

We can tell staff what to look out for, but just telling them to be curious and morally active isn't enough. It's about **confidence building** in employees.



Impact

The far-reaching consequences of fraud are widely recognised amongst RP's when discussed, however a feeling of immunity and a relatively passive approach persist across the sector. Creating an environment of transparency where fraud is openly discussed, and its impact acknowledged is crucial in shaping perceptions and behaviours.

Ignorance is not bliss

It is often the knock-on effects fraud can have on an organisation that are often overlooked. Where financial loss is often first to be addressed the impact on employees and the erosion of trust can 'rock' a workforce, damaging morale and leading to decline productivity, service levels and disruption at an operational level.

How many instances of fraud are not being defined as fraud or reported as fraud? Why aren't RP's focusing more on 'near misses' to get ahead of the game in the same way action is taken to improve H&S performance?

If the regulator fails to expand on nil reports, this means the sector has to self-motivate to look for the steps that need to be taken to firstly convince, and secondly educate, colleagues across the sector of the growing threat of fraud and the benefit to taking those actions.

In our view, there seems to be an unfair, unfounded expectation that the responsibility starts and ends with certain roles in each organisation when it really does not. It is a collective 'look-out' for all working at each RP. Greater due diligence and education is needed, along with a wider culture of ownership across organisations that appreciates the need for a more proactive stance.

Prevention

Can we say confidently that enough is being done when it comes to preventing fraud and what does good look like?

One of the key answers is people. A phrase has evolved in the counter fraud world discussing our human firewalls using their human intuitive controls: their eyes and ears being those of your organisation. If they know what to look for, they will find it. That might be finding a risk or finding wrongdoing, but if you do not know what you are looking for, you cannot find it. This is a factor that often goes underappreciated. Yet many businesses and employees alike are under-resourced, over-reliant on internal audits, or uncomfortable with whistleblowing and promoting constructive curiosity.

Many people don't understand what to report, feel that they have the time or perhaps in some cases, why they should, feeling that systems are about 'telling on' others rather than as a means to collectively prevent and protect (social housing/charitable assets).

Changing the language we use and the perception created is one way to reduce the pressure and intimidation and promote an environment where people are encouraged to speak up.

It starts with employees understanding why they are being educated about fraud: to help protect themselves, their families, and their employer. This helps foster an environment where employees feel more inclined to be curious and report any concerns. Providing clarity on how the functioning of a whistleblowing policy right from the start can help dispel stigma and reshape the perception. By reframing it as an opportunity in whistleblowing rather than a negative by saying it is a portal to not just report bad actions but an avenue to help identify when your people see risks in the organisation, individuals and senior management teams can better understand its potential benefits.

Internal fraud is harder to accept. When it's a long lasting employee, **nobody ever expects it to be that person**, but circumstances change and people know where the opportunity is.

Other thoughts on prevention include:

- **Awareness** – more signposting to events, insights and resources
- **Digital learning** – overcoming the challenge of mass face-to-face training
- **Education** – individual case studies and quizzes can help drive new values
- **Feedback** – having employees say how they see fraud risk in their specific roles
- **Risk register** – language, analysis, transparency
- **Best practice** – a basis to work from followed by up-to-date thought leadership
- **Mystery shopper** – bring someone in to test controls as we do with cyber testing
- **Technology** – work with AI, technology and the digital community, not against it

Emphasising the importance of awareness and education for both new recruits and the ongoing re-education of existing staff is paramount. It is imperative to adopt a consistent and continuous approach to fraud prevention rather than relying on isolated incentives. An annual focus falls short in reflecting the gravity and scope of the issue.

Any complacency surrounding fraud should be dispelled, especially in critical business departments such as finance, supply chain management, development, housing management, as well as within human resources and the internal communications team. These departments play a pivotal role in delivering the anti-fraud messaging and ensuring its lasting impact.



Wider issues for ARC

Generally, should the attention given to fraud be more of a focus for Audit & Risk Committees? As already discussed, often the areas considered are limited to some key areas. Assurance on the back of Internal Audit activity, common internal control frameworks or reliance on key accreditations (such as Cyber Essentials) usually allows fraud to have low residual risks on Risk Registers. Meanwhile, there tends to be limited discussion relating to near misses and noting of annual nil returns to the Regulator, which are met with limited wider guidance beyond basic procedure and a short reference to fraud in the regulator's annual Risk Sector Profile (2022 – included briefly and at a high level within sections 5.15 to 5.17). Does this lack of emphasis, or perhaps unconscious downplaying of fraud risk contribute to normalisation?

A scenario where we could inform the Regulator and work more collaboratively is a potential avenue to explore. A firmer, less passive approach from the sector would be needed. However, in return, RPs all need to feel like reports are being read and taken seriously with an expectation of collective feedback to the sector being forthcoming year on year. This would enable them to learn from each other and continue to develop preventative skills – fostering a unified approach in the sector.

Data is key here, and severely lacking at present. To be proactive, we need better data extraction and analysis to become a formal prerequisite of fraud prevention – even if it's anonymous. While a freedom of information request on the RSH asking about the data in these returns might be too confrontational, we advocate for building greater sector-wide awareness in a co-regulatory approach with the Regulator as we believe it would hopefully see the Regulator promote a consistent and cooperative approach year on year to enhance learning and improvement.

“We should lead with the language of keeping customers, homes and our organisations safe, rather than ‘we know you're up to something’”





Benefits

What should our motivations be for better fraud prevention? What does the sector gain other than what the sector can save in terms of cost and reputational harm. After all, prevention opens up a plethora of opportunities beyond the net savings being missed by accepting fraud as the cost of doing business.

Fraud prevention has the power to protect social housing assets and keep staff and customers safe – in and outside of work. Education around the issue can genuinely benefit people's lives, creating a strong social value element from a proactive approach. What's more, staff are likely to feel more connected to a business that takes steps to protect them – giving something real, positive and impactful to talk about in relation to ESG, encompassed by the sector's Sustainability Reporting Standard.

This moral aspect should be a strong driver for sector organisations and the regulator, and it could help form the basis of future co-regulation.

So, what's next?

A common desire to improve fraud prevention has further invigorated our ambition to bring continuity to this conversation towards better regulation and more proactive approaches. We've collated a set of potential best practices to act as a starting point for improvement.

Best Practice Guide

Suggested routes to drive change

Invest in awareness

- ✔ Stories are the best form of education – bringing to life the shades of grey where fraud has occurred is vital for engaging employees on the subject.
- ✔ For more senior members of your team, this approach ought to be backed up with data and software, as this will be key to identifying, protecting against, and preventing fraud on an ongoing basis.
- ✔ Seek to embrace technology and harness digital capabilities across the fraud spectrum.
- ✔ Embed an awareness of different fraud types and how these can manifest within employees' day-to-day lives.
- ✔ Link other areas, like safeguarding and anti-loan shark procedures, together with fraud to demonstrate how they relate and make them stick.
- ✔ Reposition fraud prevention in people's minds as a genuine social value benefit, and something to be gained both inside and outside of the workplace.
- ✔ Be proactive in the improvement of lives and experiences, leading to a better anti-fraud culture as a result.

Educate your people

- ✔ Implement a robust but engaging staff training policy that is regularly refreshed in line with the changing fraud landscape – particularly around when a member of staff is promoted or moved to a different role.
- ✔ Ensure employees are engaged on the subject of fraud and what fraud translated to in the context of your organisation's operations.
- ✔ Incorporate digital learning to save the costs and resources associated with mass face-to-face training.
- ✔ Lead with the positive language of keeping customers, staff and clients safe – particularly in the context of making employees feel comfortable with the idea of whistleblowing, e.g. renaming it as a 'speaking up policy'.
- ✔ Do not exclude your tenants or suppliers from the learning journey – engage with them to educate about fraud as they too can be your eyes and ears. Talking about fraud is a deterrent, which is important to remember.

Refine your approach

- ✔ Information sharing is too hard when you tackle the whole spectrum. Focus on digestible or palatable areas first to give people something they can get behind.
- ✔ Explore the potential of how mystery shopping/fraud testing could work as a means to understand how vulnerable – or well protected – your organisation is and identify areas for improvement.
- ✔ Support RPs to collaborate more effectively using common support organisations such as TFF and FAP, as well as getting involved with National Charity Fraud Awareness week in November.
- ✔ Consider sharing trend analysis from fraud reporting with others in the sector.

The state of play – Best Practice across the Sector

Examples from the sector of good practice, areas for improvement and further investment to help combat fraud

Consolidate Best Practice

- Financial controls (Payroll, AP, mandate, Supplier)
- Procurement
- Cyber
- Housing (Application, RTB, Succession)
- Customer (Anti money laundering, Anti loan shark)
- Maintenance (stock and fleet management)

Greater progress needed

- Tenancy Fraud (short and long term lets)
- Development
- Training and Awareness
- Fraud testing (similar to IT third party testing)
- Conflict of interest checking/Collusion
- Stock management (maintenance companies)
- Disrepair claims
- Customer (Gas capping scams, Digital)

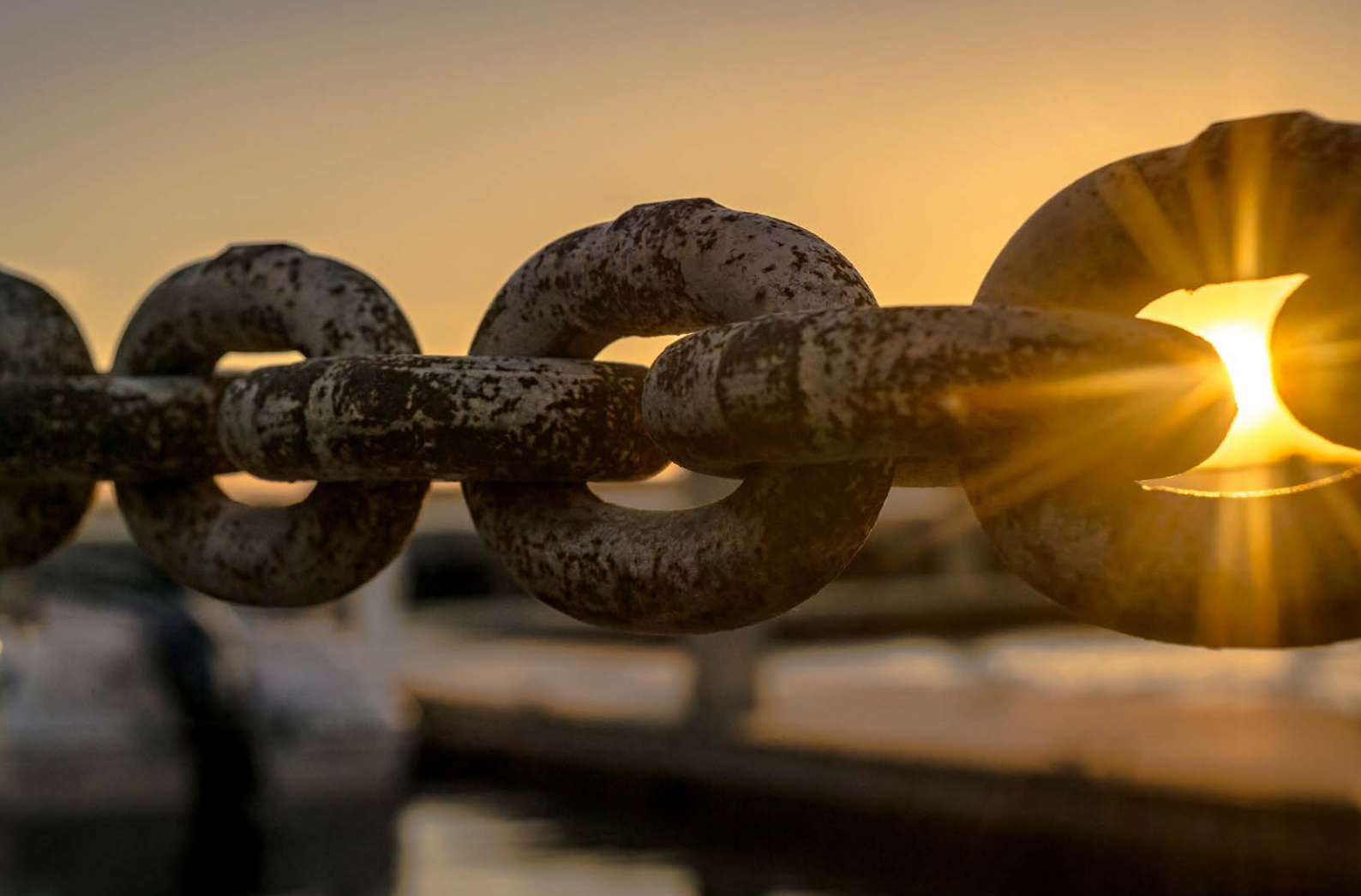
Investigate Further

- IT (cyber and AI)
- Support for customers and colleagues
- Former Tenant Arrears
- Professional Services (sharp practice)
- Maintenance Services (accreditations, Esg credentials)
- HR (misrepresentation, critical roles)

Our joint offering - Get in touch for training and support

Arun and Paul have developed targeted training for Audit & Risk Committees and Boards with a focus helping them to understand the challenges that fraud risks pose to affordable housing organisations and their people. This training aims to empower participants to transform these threats into opportunities by implementing changes in practices, procedures, and culture. This approach ultimately strengthens the assurance offered to the Regulator with respect to governance and financial viability.

The fixed fee training can be provided in person or remotely. A discount for the training of 10% per session is available using **discount code FRAUD...NOTHING TO SEE HERE.** The discount is only available to be used once by any registered provider.



Culture, Tools and Collaboration

Our aim is to help better protect people, assets and reputation across the sector and this whitepaper is just the beginning.

Addressing the rising fraud risks in Registered Providers is critical. Ensuring these concerns are integrated into your Audit and Risk Committee's agendas and risk registers is essential. Horizon scanning and seeking innovative solutions to protect affordable housing assets and enhance their social impact will enhance your organisation. Together we can challenge the norm of why fraud risk and impact isn't talked about more across the sector.

Through collaboration, webinars, events, thought leadership, education and awareness we are striving to share best practice to improve your grasp of fraud-related challenges, helping to evaluate the strength of your anti-fraud culture to safeguard your assets and maintain trust.

Sign up to our marketing list

SCAN ME



Join Our LinkedIn Community Group today to learn more

SCAN ME





tenet