January 2025

Specialty: What's Alive in 2025

January 2025

The Forecast

Now is the perfect opportunity to forecast the trends and risks we anticipate going into 2025 drawing upon our experiences in 2024 and offering our thoughts on how best to avoid and mitigate future claims and new risk areas for your business and the customers we all service.

We've taken each line of business within our Specialty portfolio highlighting the specific claims issues and trends for each line with key take aways and our thoughts around risk mitigation and avoidance.

Professional Indemnity

2024 was a busy year for those of us handling professional indemnity claims, the regulatory and legal landscape for all professions is changing at pace. Above all, 2024 will be remembered for Grenfell due to the publication of the Phase 2 Report, but also for the Post Office scandal both of which have shown how critical it is for an organisation to have a clear set of values and behaviours, which foster a positive culture to empower people to do the right thing at the right time. We think this must, should and will remain at the forefront in 2025. A positive culture within an organisation is a risk manager's most useful tool in their arsenal when it comes to tackling risk and claims mitigation.

Construction

The key trends which have previously impacted this industry remain a continued presence as we enter 2025 - claims inflation and insolvencies. The combination of high interest rates and labour shortages as well as the new building control processes, introduced by the Building Safety Act ("the BSA") with the creation of the Building Safety Regulator, has directly impacted the cost of remedial schemes and the levels of damages which Claimants are pursuing.

To fund remedial works, we anticipate an increased focus, by a much wider pool of Claimants, on the types of remedies available under the BSA, such as, Remediation Contribution Orders and Building Liability Orders. The new Labour government has also recently announced a 'new remediation acceleration' plan with tough new targets to fix unsafe buildings quicker with clear target dates and tougher penalties for those refusing to act.

According to data released in September 2024, by the Ministry of Housing Communities & Local Government, approximately 4,821 residential buildings, 11 meters and over, have been identified as having unsafe cladding. Remediation works have been started on less than half of buildings and completed on less than one third of buildings, identified as requiring remediation. As developers complete both their assessment of buildings and remedial works, we may expect more 'fire safety related' claims to be brought in respect of legacy projects and predict some knotty times ahead as Insureds, brokers and Insurers grapple with what has been notified to date and whether further notifications are required.

As the construction industry, Insurers and Courts get to grips with the new statutory liabilities created by the BSA, we have seen Claimants revert to old ways and commence Adjudications. We expect this trend to continue into 2025, Adjudications are relatively quick, less expensive than formal proceedings and if successful, cash flows are strengthened as damages will have to be paid promptly, in turn, increasing the focus on insurers to confirm policy cover. In these circumstances, we recommend that Insureds provide as much information as possible to their Insurers, including a copy of the Building Contract/Appointment, the Referral Notice and expert evidence on both liability and quantum, to enable a coverage investigation to be undertaken quickly.

The industry continues to digest the long-awaited Grenfell Phase 2 report, which was released on 4th September 2024 alongside a public statement from Sir Martin Moore-Bick. Given the findings made, we anticipate there may be sharper focus on the role that architects and manufacturers played in connection with cladding decisions and that they are likely to face further scrutiny over their conduct. Indeed, the Architect's Registration Board has issued a note advising that they have published a draft version of a revised Code for consultation. The current code was published in 2017 and amongst other things, the proposed revisions are intended to capture the recent developments in building safety.

Reports in 2024 suggested the construction industry was struggling with the new building control processes, introduced under the BSA, a significant number of building control applications have been rejected by the Building Safety Regulator for failing to meet requirements due to a lack of information. This, in turn, delays progress with remedial works and leads to higher costs. It is, therefore, imperative, that Insureds put in place proper policies and practices to 'get it right first time', ensuring through training that they understand the changes to the building control process, that they are providing the right drawings and that they can demonstrate upfront how a building will meet requirements. Insureds will need to work closely with their supply chain to ensure everyone is aligned, requests for documentation are made timeously and any avoidable delay is minimised. A good document management system is essential. This is not only important during the lifetime of a project but also a full and complete set of documents is crucial to successfully defending a claim post completion or, indeed, during a project.

The Phase 2 Report made several recommendations. It remains to be seen which ones will eventually be implemented. There may well be further amendments to the BSA including, potentially, redefining a 'higher risk' building.

The construction industry will be watching closely and will need to remain agile and able to respond to the changing legal and regulatory landscape to ensure compliance. One of the issues central to the Phase 2 Report was a lack of accountability. Insureds need to sharpen their focus, pre-contract, to ensure that they are clear about their own contractual obligations and those of their supply chain, that they have carried out suitable due diligence on their supply chain, particularly around solvency, insurance cover and expertise and that they have appropriate caps on liability, to effectively manage risk and to continue to operate in a new regulatory environment. Finally, Insureds need to ensure that they are building a workforce fit for the future which is innovative and competent for an evolving legal, regulatory, and physical environment.

Solicitors

As organisations continue to adapt to the new working landscape with hybrid working, increased use of digitisation and labour shortages, law firms remain vulnerable to data breaches and to financial crime, such as, theft and fraud in relation to client monies. These are trends which we have seen and when we dig into the primary cause of these claims, it is often a lack of oversight and supervision, blurred reporting lines and frequently the lack of training of non-legal staff about remaining vigilant for any unusual requests for payments or changes to client account details.

Cyber resilience must remain a key priority as part of a firm's overall risk management strategy, with thorough training provided to all

employees about the harms caused by cyber-attacks through phishing and other forms of social engineering and how to identify and avoid these risks. Resilience and preparedness are key strategies for mitigating risk and tackling threat actors who are increasingly sophisticated and quick to adapt to any measures put in place to prevent a cyber-attack - more details and practical guidance below under our "Cyber" section.

In relation to supervision, whilst there are many benefits to remote working, the downside is the potential risk of individuals working unsupervised or in silo, if a collaborative working environment is not positively promoted to ensure all employees feel supported and confident enough to speak up if something is not going well. Similarly, a good case management system is vital to ensure that documents are properly maintained, managed, and stored and that diary dates are not missed.

The digitisation of the Court system and the introduction of online portals increases the risk of a claim based on user error. As firms fulfil obligations around ESG, care must be taken to ensure that any pro bono work carried out is carried out to the same high standard as fee earning work.

We have seen a shift away from assessing risk based solely on different work types within a firm, law firms need to take a more holistic approach to risk. The SRA is tightening its grip, with higher financial penalties as it tackles consumer protection, particularly around preventing economic crime and the ethical behaviour of, and within law firms, following the Post Office Horizon IT Inquiry and several high-profile law firm collapses after mergers. As The Law Society consults on whether firms should continue to hold client monies, these regulatory themes will continue in 2025.

Accountants

We are still awaiting the implementation of a new audit and governance regulator, the Audit, Reporting and Governance Authority, which was introduced following several high-profile corporate collapses. The proposed reforms include improving the quality of audit reporting and encouraging competition and choice within the audit market and it is likely that the Audit Reform and Corporate Governance Bill will become statute this year. With the increasing number of insolvencies, there will be increased scrutiny of Auditor's work.

Records show that one in 179 companies on the Companies House Register entered insolvency between 1 July 2023 and 30 June 2024. This equates to a rate of 55.8 per 10,000 companies and is an increase on the previous 12 months when 55.1 per 10,000 companies entered insolvency. In turn, this leads to more claims against insolvent companies' professional advisors including accountants and auditors, as insolvency practitioners carry out more investigations. We have seen the FCA recently impose a fine against PricewaterhouseCoopers (PwC) for failing to report to the regulator their belief that London Capital & Finance plc might be involved in fraudulent activity. This is the first time the FCA has fined an audit firm. Another example is the recent decision of again PwC's auditing arm being suspended from China for 6 months for its work on the collapsed Chinese property giant Evergrande. They were also fined $62m. Both examples highlight an increased focus on auditors to report any evidence or red flags which indicate fraud. Failure to do so will lead to serious repercussions for those firms, not only fines but also possible suspension.

The Economic and Corporate Transparency Act 2023 (ECCTA) created a new corporate criminal offence of 'failure to prevent fraud'. Under the new legislation, an organisation will be criminally liable where:

- a specified fraud offence is committed by an employee, agent or other 'associated person', for the organisation's benefit
- the organisation did not have 'reasonable' fraud prevention procedures in place

It does not need to be shown that company managers ordered or knew about the fraud. The offence applies to:

- all large incorporated bodies, subsidiaries and partnerships

- large not-for-profit organisations such as charities if they are incorporated
- incorporated public bodies

The offence will come into effect on 1 September 2025.

The decisions highlighted here and ECCTA demonstrate an increasing need to ensure the appropriate risk management procedures are in place within all organisations and will be of particular focus for auditors and accountants. The best way to ensure this is to ensure that the firm in question has the correct quality management standards in place, peer reviewing of files, a culture which allows for quality and accountability and ensuring staff are trained on the key risk areas.

In October 2024, we saw the first labour budget in 14 years. The budget made various changes to the tax landscape which could potentially increase the risk for any professional advisors in tax planning. We are also likely to see pressure on small businesses because of the increase in Employer's National Insurance Contributions which impact insolvencies and potentially expose any professional advisors acting immediately before the insolvency to risk.

The ICAEW, the largest professional body for accountants, has announced several significant changes to its PI insurance requirements. The changes include the increase in the minimum level of cover from £1.5m - £2m. The changes also include amendments to the definition of a "large firm" not requiring qualifying insurance as well as changes to the calculation of excesses.

Surveyors and Valuers

Following changes to the 2024 RICS Minimum Approved Wording, the enhanced fire safety cover, available from 1 July 2024, hints at a degree of optimism surrounding future fire safety exposures.

However, Part 4 of the Building Safety Act has introduced a new system for managing safety in occupied higher risk buildings through the creation of a new statutory duty holder for such buildings. The Building Safety Act imposes several statutory obligations on the Accountable/Principal Accountable Person - in some instances, a breach will be a criminal offence – which are intended to strengthen practices around building safety. This includes an obligation to prepare a Safety Case Report which is crucial in reducing the risk to life safety in the buildings.

A Building Safety Case Report is a document which outlines the potential risks to fire safety and structural integrity are identified, managed, and mitigated. The main aim of the Safety Case Report is to show that the accountable persons have assessed any major fire and structural hazard/risks and created strategies to manage and mitigate these risks.

The government has provided guidance on preparing a Building Safety Case Report but no specific examples of what the report should look like. This potentially poses a risk to anyone responsible for preparing a Building Safety Case Report and they should be familiar with the requirements of the Report which will include a description of the building, for example, the height, number of floors and staircases, information about who will live in the building, and the building risks which have been identified and how these are being managed. This means having a familiarity with the building which is the subject of the Report and ensuring that the Report is kept updated. The Building Safety Case Report is a critical document in the on-going statutory obligation to keep people safe.

We anticipate that Property Managers will be asked to agree to act as the Accountable/ Principal Accountable Person which may present a risk if those individuals have not had the requisite training and experience so moving into new areas needs to be undertaken with caution and clarity around the scope of duties assumed.

AI and professional services firms

The benefit of AI is recognised by many firms across different industry sectors. Examples of its use can be found in the financial sector in the management of equity funds and fraud detection; in the legal sector to assist with disclosure and the preparation of trial bundles; the property sector to streamline processes and connect with clients through better targeted marketing; architects to predict energy consumption/ sustainability indicators under different design scenarios; and in many other ways.

AI can analyse vast amounts of data, streamline operational tasks, save huge amounts of time and therefore cost. If used correctly, removing laborious data review and document heavy tasks allows organisations across all sectors to focus on the more human and creative elements of its specialism leading to an enhanced customer (and employee) experience. In theory you would think this would minimise risk as so many of the claims we see, and handle arise from simple human error. However, with all the benefits of AI also come challenges and risks that need to be carefully managed throughout the AI cycle.

The liabilities arising from the use of AI will impact organisations differently depending on the nature of the business. To prevent the sort of liabilities that could arise from using AI organisations will need to invest time and money at each stage of the AI cycle. Although most organisations will only ever use AI as part of a licensed, third-party product they should still have appropriately skilled teams in place to ensure that potential liabilities that could arise at the early input stage are identified, understood, appropriately managed, and documented. Some organisations will have the technical resources available to do this internally and some will need to rely on third parties (such as legal advisors).

The importance of organisations investing time and seeking appropriate technical legal advice in the early stage of AI deployment cannot be understated when it comes to managing AI risks. Organisations that tackle the issues head on, have clear user policies in place and offer good training to its stakeholders will be best placed to prevent exposure to costly claims and enjoy its benefits. In addition, businesses need to actively engage with their customers around their AI use and be clear as to where it's being utilised as well as remembering the importance of human interaction and engagement to the customer experience.

The use of AI across all professions will continue in 2025 and we are likely to see new risks emerge if the proper checks and balance are not in place, particularly where human oversight has been removed from a task.

Cyber

Now is the perfect opportunity to address the trends, risks, and legislative changes we foresee in 2025, mindful that Cyber is an extremely fluid environment. Firstly, it's important to start with the legislative changes as detailed below.

Legislative changes in the UK and Europe

Cyber Security and Resilience Bill

This new bill was announced during the King's Speech in July 2024, stated to be a response to the increasing frequency of attacks by cyber criminals affecting essential public services and infrastructure, and is due to be introduced to the UK Parliament in 2025. Following the recent updating of the 2018 EU Network and Information Systems Regulations (NIS) in 2024, the intention is for the UK efforts to be aligned with the EU regulations by expanding the remit of the regulation to protect more digital services and supply chains, putting regulators on a stronger footing to ensure essential cyber safety measures are being implemented

by organisations, and mandating increased incident reporting to give the government better data on cyber-attacks.

EU Digital Operational Resilience Act (DORA)

DORA is an EU regulation which becomes fully enforceable on 17 January 2025 and as such does not need to be transposed into the national law of a Member State. DORA focuses **exclusively** on the financial sector and applies to banks, insurers, investment firms and other providers of financial services in order to safeguard economic stability and protect against systemic risks caused by digital threats. The rules relate to classification and reporting of Information Communication and Technology (ICT) related incidents, resilience testing of ICT tools and systems, ICT risk management framework, third-party risk management, and threat information sharing. Supervision of compliance with DORA is primarily carried out by national authorities, working closely in conjunction with EU Authorities such as the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA). Firms that violate DORA's requirements are potentially liable to fines of up to 2% of their total annual global turnover. In addition, members of senior management can be held personally liable for gross negligence or wilful misconduct and can face a maximum fine of EUR 1 million.

EU Network and Information Security Directive (NIS2)

Being a directive, it is up for individual Member States of the EU to enact their own legislation to embed the necessary measures to achieve the general objectives of NIS2 into national law. The deadline for implementation passed in October 2024 so any companies operating in certain sectors within the EU will need to ensure that they are compliant. The three fundamental pillars of NIS2 are defining national cybersecurity strategies, requiring certain companies to take appropriate security measures (with accountability for non-compliance), and support for strategic cooperation and exchange of information between Member States. The Directive is specifically aimed at companies and organisations in several critical sectors which are essential to the functioning of society and the economy, such as transport, healthcare, water supply, and energy. Under NIS2, 'essential entities', such as those in energy, transport and healthcare sectors can be fined up to EUR 10 million or 2% of their global annual turnover (whichever is higher). For 'important organisations,' such as digital service providers like search engines, cloud computing services, and online marketplaces, the maximum fine is EUR 7 million or 1.4% of the global annual. As with DORA, senior management can be held personally liable for failure to comply with the directive.

Artificial Intelligence Regulation

Back in 2023 a Private Members' Bill was introduced in order establish an AI Authority to oversee the regulatory approach to AI in the UK. However, despite garnering a great deal of support, this was scrapped because of the announcement of the General Election. It remains to be seen the extent to which the new government wants to apply regulation to the rapidly advancing field of AI, but early indicators are that if new regulations are created, these will represent a more light-touch regime than the types of prohibitions set out in the EU AI Act.

State-backed Cyber Reinsurance

Pool Re, which is a terrorism reinsurer working in partnership with the UK government and has been in operation since 1993, is set to present proposals for a systemic cyber insurance pool to the new UK government in the early part of 2025, which was discussed at the recent Ferma Forum in Madrid. The government response to the proposals will be eagerly anticipated, but it should be noted that the Office for Budget Responsibility has previously cast some doubt on the viability of a such an insurance pool. Having noted in 2022 that the terrorism scheme has never called for the government guarantee, they comment, *"this is not to suggest that in the event that signs of weakness in the cyber insurance prompted a similar intervention, a parallel scheme would be equally resilient. Given Pool Re has had*

nearly 30 years to amass the reserves now able to absorb significant future losses, the more imminent threat of cyber risks, and the potentially high impact of a catastrophic attack could combine to make an unlimited exposure to this risk more fiscally challenging than terrorism risk has proved to date."

Crowdstrike

One of the most significant issues in 2024 was the Crowdstrike outage, caused by a defective software update, which affected approximately 8.5 million Windows devices, and led to significant disruption to organisations across the world, across a wide number of sectors. It is estimated that the insured losses from the outage will potentially reach $1.5bn. The losses flowing from the outage outlined the fact that companies need to have cyber policies which respond to system-failure losses as opposed to just losses caused by external malicious attacks by threat actors. We would expect policyholders and insurers to be reviewing their wordings and coverage even more carefully as a result of this incident in 2025 and be tightening up their own disaster-recovery policies given the widespread disruption caused to many organisations.

Threat Actor Fragmentation

2024 saw law enforcement authorities having success in combating threat actor groups including ALPHV/BlackCat, Hive and LockBit. Whilst this is ostensibly a good thing, this hasn't reduced the overall frequency of cyber-attacks, when threat actors can easily rebrand themselves and may make it harder to predict behaviours based on previous dealings leading to a more cautious approach being necessary when negotiating ransoms during 2025.

Change of Extortion Tactics

Often, in so far as extortion is concerned, data exfiltration has been the main extortion lever rather than any operation disruption, with no ransomware actually being deployed. This is perhaps the result of the prevalence of backups being more common as a mode of negating that tactic. As a result, we may find that data theft, leak sites and the publication risk will become the main focus of an organisation's response, over any operational impact. However, it is important to be mindful of a potential change in tactics by cyber criminals to combat this. One change is possible physical threats. Organisations now, therefore, need to be aware of not only the operational risk of a cyber-attack but the potential personal risks which may be faced, and take appropriate steps to safeguard the people involved.

Increasing Sophistication of Gen-AI Assisted Deepfake Fraud

A big talking point in 2024 has been AI and how its use can be regulated as touched on above. AI has infiltrated many areas of society already and, whilst it can create benefits, it most certainly also creates risks as addressed in our Professional Indemnity section above. Concerns associated with gen-AI assisted deepfake fraud have been shared by the Solicitors Regulatory Authority, which has warned lawyers of the risks posed by deepfake technology, and Interpol's financial fraud assessment warning that organised crime groups are increasingly using AI, large language models and cryptocurrencies combined with phishing and ransomware-as-a-service business model to commit fraud campaigns at relatively little cost.

One particular example of the risk of AI was the report in May 2024 of a Hong Kong subsidiary of a British company falling victim to a convincing deepfake fraud, resulting in a loss of HK$200m. This is the world's biggest known deepfake scam. It is reported that the fraudsters used generative AI to create digital masks and voice emulators of the firm's CEO and financial director, enabling the fraudsters to appear as said individuals on a video conference call with the firm's finance department. The result? They convinced the employee in the finance team to make 15 transfers which were said to be urgent and confidential. This came only a week after the world's biggest advertising group was also targeted in an elaborate deepfake scam.

The fraudsters utilised video and audio clips from the real CEO and financial director to create the digital masks, as such, it is important for companies to consider which senior officials appear in publicly available videos and recordings, given the sophistication of the deepfake fraud which has been witnessed this last year. Strict procedures should be in place, alongside relevant training, governing what employees should do in situations where senior staff members ask them to make urgent transfers. Many companies are aware of and provide training to employees with regards to email phishing scams. Therefore, due to increasing sophistication and impact of generative AI, companies should urgently review their training programmes and make appropriate changes. Whilst this impacts all companies, it should be of particular focus for large corporates who will need to ensure they have adequate fraud prevention measures in place once reforms come into force under the Economic Crime and Corporate Transparency Act (ECCTA).

Business Email Compromise

Business Email Compromise (BECs) is a type of cybercrime where a fraudster gains unauthorised access to an organisation's email account. This is done by using a legitimate user's credentials, which are most typically obtained via phishing campaigns or purchased on the dark web.

BECs dominated the cyber landscape in the latter part of 2024, and we expect them to continue to be prevalent in 2025. Criminal tactics are becoming more and more sophisticated with BECs becoming more targeted and convincing. Attackers are circumventing traditional forms of multi-factor authentication (MFA), which poses a further challenge for organisations to prevent, identify and stop these types of attacks. The activities undertaken once an attacker has access to a mailbox can result in significant consequences for an organisation, including reputational damage, both direct and third-party losses, and heightened regulatory scrutiny.

Whilst no security controls can provide complete protection against a BEC, the risk of a BEC can be reduced by organisations taking several measures to protect themselves both before and after an event. This includes regular phishing awareness training and simulation exercises, setting up Domain Message Authentication Reporting (DMARC) to prevent unauthorised parties from sending phishing emails using their domain, disabling the ability of external parties to start chats with users on Teams and monitoring the dark web for any credentials which are leaked, to name a few.

In addition to these steps, whilst MFA makes a big difference compared with reliance solely on passwords for authentication, this must be enforced on a mandatory basis. Even with this in place, a number of social engineering techniques aimed at obtaining passwords can be updated to overcome some methods of MFA. The National Cyber Security Centre (NCSC) has recently updated its guidelines to enable organisations to choose the strongest type of MFA which is most practical for them. We would therefore strongly urge organisations to consider this guidance to ensure they are utilising the most appropriate MFA for their business.

Types of cyber-attack developing

What types of cyber-attacks do organisations need to be aware of, in 2025, and what is the associated risk of these? The European Union Agency for Cybersecurity (ENISA) recently published a report which sets out the prime cybersecurity threats. Whilst many of these are not new, this demonstrates that the risks already identified remain in 2025:

- Ransomware – noting several high-profile and highly publicised incidents in 2023/24.
- Malware.
- Social engineering – various forms of manipulation are being used to trick victims into making mistakes or handing over sensitive or secret information. Users may be lured to open documents, files, or e-mails, to visit websites or to grant access to systems or services. With the advent of AI tools, the risk of fraud, counterfeit, and impersonation as part of this risk is growing, particularly as part of considerations

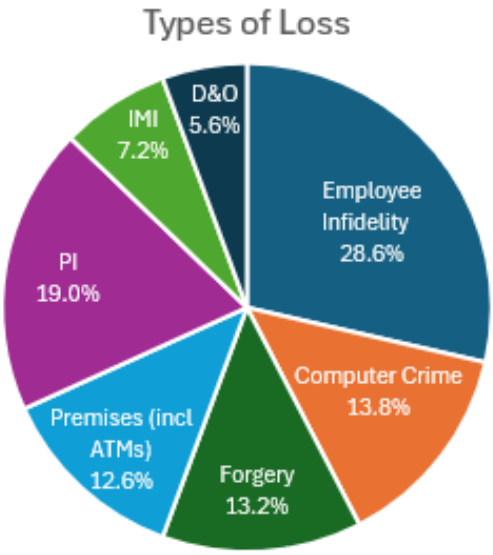
of cybersecurity. ENISA noted that "*the threat of AI-enabled information manipulation has been observed, but still on a limited -albeit evolving - scale. For example, some threat actors are experimenting with AI for information manipulation seemingly to assess how AI can be exploited in this context*." Threats against data.

- Threats against availability: denial of services.
- Information Manipulation.

Cyber risks continue to be of concern in 2025 with the legislative changes highlighted above reflecting this. The high-profile cases of 2024 provide valuable insight into the tactics being adopted by cyber criminals, the risks organisations face and, as a result, identify those areas where improvements can – and must - be made. We will no doubt continue to hear of cyber-attacks regularly within the news as attackers become more skilful, placing many organisations at risk of suffering from a cyber event and, potentially, an exposure to claims. It is imperative that organisations continue to keep abreast of the ever-evolving landscape and ensure they have the best systems and policies/procedures in place so they can limit cyber-attacks and the effects of these which, as we are all aware, can be both costly and damaging. In addition, organisations must ensure that they have the necessary levels of insurance cover in place to deal with this ever-increasing threat and risk exposure.

Financial Institutions and Directors and Officers

Our loss adjusting colleagues at ASL have recently shared their market wide statistics on the types of loss they are seeing across the Financial Lines landscape, and this is a great place to start when reflecting on what's been seen in 2024 and what we anticipate for 2025.



As you can see from the chart, Employee Infidelity is still the highest-ranking loss type, while PI loss is the 2nd largest source of losses at 19%. Crime losses have dominated the financial lines landscape this year and understanding these trends and forecasting what the future holds is crucial for Insurers when pricing new and existing business and for customers when considering the risks to their business and the level of cover and protection required. Whether it is applying a smaller limit of indemnity throughout, sub limit to certain sections of the cover or inserting higher or lower deductibles compared to the previous year, it is critical that the cover is both fit for purpose for the business. While each policy is looked at on a case-by-case basis, data can be used to pinpoint the types of loss that are most likely to occur and give us an idea of potential quantum which in turn can guide Insurers, brokers, and customers on the scope of cover.

In terms of 2025, we can certainly surmise that Employee Infidelity will continue to be a large source of loss within Financial Lines. The keys to avoiding these types of losses are strict controls around the handling of physical currency inside and outside of branch/business, while also ensuring that there are stringent controls in handling customer accounts, both day to day retail customers and high net worth customers. Another way to help avoid potential losses under employee infidelity is to educate the customer regarding the processes they will be subject to for their

banking activities, including dual authorisation and call backs – our Cyber section above also highlights some of the risks here and offers risk prevention advice.

In terms of professional indemnity losses, many of the themes and risk avoidance tips in the "Professional Indemnity" section have equal application to our Financial Institution customers. It is essential that businesses ensure employee training is kept up to date in terms of processes to follow to avoid any critical mistakes that puts the Insured and customers at risk of loss. Professional indemnity losses; while not as common as employee infidelity; do carry a higher average quantum (approximately double) demonstrating why education of staff is so vital to avoid errors. Increases in the number of professional indemnity losses within the Financial Lines space will only serve to increase premiums given the higher quantum these losses exhibit.

We anticipate that we will continue (as we have in 2024) to see increases in ATM losses. Most emanated from Eastern Europe, Latam and other jurisdictions where day to day society remains mainly cash based. Although smaller in value, this type of loss adds up especially if a certain criminal gang decide to target various Insured ATMs in a short period of time.

Motor Finance - Discretionary Commission Arrangements (DCA's)

After a busy 2024 in this area, we anticipate a further uptick in claims in 2025 arising from car financing secret commissions, impacting car financing lenders and maybe their D&Os, with the potential knock-on effect for other professions and businesses where commissions are charged. This is very much an area to watch and keep a close eye on.

By way of a recap, in April 2024 the FCA warned various lenders about potential future redress from customer complaints that may arise out of the FCA's Section 166 FSMA review into historic DCAs. This began in January 2024 following two successful FoS complaints that found customers were treated unfairly due to the lenders failure to disclose the commission arrangements. DCAs entitle brokers to set the rate of interest on a car finance loan provided to a customer and receive a commission directly based upon the interest rate set. Previously the general assumption was that a car dealer providing point-of-sale finance was not in a fiduciary relationship with the customer.

In October 2024 the Court of Appeal handed down their decision on the joint appeal of three secret commission claims in which the Claimants succeeded (Johnson -v- Firstrand Bank Limited, Wrench v Firstrand Bank Limited and Others, Hopcraft -v- Close Brothers Limited [2024] EWCA Civ 1282) finding as follows.

Where a commission is kept 'wholly secret' it is sufficient to give the borrower a remedy against the lender as a primary wrongdoer, provided the broker owes the Disinterested Duty – a fiduciary duty is not needed. That remedy will include as of right the ability to rescind the contract.

Where the commission is only 'partially secret', a fiduciary duty will be needed to obtain a remedy against the lender. In that instance, the lender is an accessory to the car dealer's wrongdoing.

A mere statement in the agreements T&Cs does not necessarily get over the hurdle of secrecy. The appeal court commented "Burying such a statement in the small print which the lender knows the borrower is highly unlikely to read will not suffice."

The defendant banks were recently granted permission to appeal to the Supreme Court and this should be heard before the end of the first legal term (16 April 2025). However, pending the appeal the outcome of the above cases has increased the scope for claims arising from an intention to protect the consumer. The FCA investigations remain on-going, and they have indicated their intention to use s.166 of FSMA to determine whether there has been any widespread failure to comply with lending requirements. This is a very costly process and in turn could lead to individual investigations into Directors and Officers.

The outcome of the test cases has been reported to cause shares to go down by 15% and several of the lenders involved have set aside considerable sums for potential compensation and fines arising from these commissions.

The FCA is also considering a redress scheme for consumers. The FCA have pushed back their report until May 2025 and the outcome of this report could lead to redress schemes and potential fines for multiple lenders. In 2025 the landscape around DCA mis-selling is in the balance with potential redress becoming more and more feasible. This will in turn put pressure increasing on the industry with a possible spike in claims across the FIPI and D&O sectors.

The above sets the landscape for claims arising against D&Os and securities claims. No doubt lenders are reviewing their practices and have been doing so for some time. It is incumbent upon D&Os to ensure that any provisions are adequately reported to avoid any suggestion that misleading information has been provided to their shareholders.

Group Litigation

The Litigation funding market is increasingly being used by insolvency practitioners or other stakeholders to access justice and to provide a 'fighting fund' for claims against directors.

Recently, in the case of R (on the application of PACCAR Inc and others) (Appellants) v Competition Appeal Tribunal and others (Respondents) [2023] UKSC 28 the Supreme Court held that litigation funding agreements (LFAs), where the funder receives a percentage of any damages recovered by the successful claimant, are unenforceable damages based on Damages Based Agreements (DBAs). Litigation funders had, until this judgment, proceeded on the basis that LFAs were not DBAs and did not need to comply with the statutory requirements for DBAs. Following the decision, Funders are now amending their LFAs to navigate these statutory obstacles. Whilst therefore, the PACCAR decision caused some uncertainty this is now likely to be very short-lived as greater clarity is provided from the courts or Parliament.

The Litigation Funding Agreements (Enforceability) Bill, was introduced in March 2024 by the then Conservative Government to restore the pre-PACCAR position. In the explanatory notes, the Conservative Government said: "The Supreme Court judgment rendered LFAs unenforceable. Uncertainty around litigation funding risks a detrimental impact on the attractiveness of the England and Wales jurisdiction as a global hub for commercial litigation and arbitration, and on access to justice more broadly". However, the Bill was dropped following the dissolution of Parliament on 30 May 2024. The Bill was not reintroduced in July's King's Speech, meaning the uncertainty generated by the PACCAR judgment over the enforceability of LFAs will continue. The Government will not re-introduce the Bill until the Civil Justice Council (CJC) has completed its ongoing review of third-party litigation funding which will set out the current position of litigation funding in the UK.

While the Supreme Court's Judgement in PACCAR has caused uncertainty as to the enforceability of LFAs in the courts of England and Wales, litigation funding is here to stay in the UK and globally. We therefore only see the litigation funding market and group litigation increasing. With funders and claimant law firms working together to identify new opportunities for bringing collective claims, the risk of US-style class actions for companies and their directors has never been greater, as discussed above in relation to motor finance.

Rise in Securities Class Actions

Claims under section 90 / 90A FSMA 2000 are becoming steadily more frequent in the UK, with the majority of actions filed in 2023 and 2024, albeit the volume of such claims is relatively low by comparison to the US.

The High Court's recent decision in Allianz Funds Multi-Strategy Trust v Barclays PLC [2024] EWHC 2710 (Ch) has provided some welcome guidance on reliance and other aspects of these claims. It was held that the test for reliance could not be satisfied in respect of

published information that the relevant Claimants did not read or consider at all. It also cannot be circumvented by presenting a claim based on omissions as a dishonest delay claim, which also only applies to published information. This decision strikes out the claims of 241 different funds worth £332 million, who were advancing their claims based on being adversely affected by the Barclays share price movement only, without having read published information. Whilst this may impact the number of claims being brought under section 90A, as Claimants will not be able to simply subscribe to such litigation as interested parties, we expect this will be appealed. Claims in this case worth up to £221 million remain active and will be proceeding to trial.

There have been few other judgments – including the RBS Rights Issue Litigation in 2017 and Autonomy case in 2022 - regarding the statutory causes of action, noting securities claims generally settle prior to trial. The UK class action landscape will continue to take shape as more cases are litigated in the Courts, with investors and companies alike keeping a close eye on any appeals made by the claimants in the Barclays case, as well as the rise in securities disputes. These are extremely expensive claims to defend and something Insurers, brokers and customers will need to keep a keen eye on as the costs can be very expensive.

Financial Conduct Authority (FCA) – Enforcement and Publicising Enforcement Investigations

On 27 February 2024, the FCA issued a Consultation Paper (Enforcement Guide and Publicising Enforcement Investigations – new approach). This set out the proposed approach to the public announcement of the commencement of an FCA investigation, including who is the target and what the investigation concerns. This new approach to announcements could potentially be a driver for new civil claims, as it will alert interested parties, investors (and any litigation funders) to the FCA's concerns as to the conduct at a firm.

Although the FCA will consider public interest points when deciding whether to publish the fact the investigation has started, the FCA is proposing that this will not include consideration of the impact of the announcement on the entity. We would therefore query the potential impact on an organisation's share price due to adverse publicity. Any company which is the subject to oversight by the FCA should ensure they have adequate cover for both public relations and legal costs, which may no doubt be required in the event of responding to an FCA announcement as well as interacting with the FCA and shareholders. Costs can quickly escalate where legal advisers consider it necessary to make preliminary comments on the likely outcome of the investigation, to dissuade the regulator from publishing names.

Employment Law and the Impact on Directors and Officers

The Government is making some of the biggest changes to UK employment law in decades, through the Employment Rights Bill 2024 (the "Bill"). Whilst the Government has promised to consult with business, there is no doubt these changes will have a fundamental impact on business, but also the directors and officers of these businesses.

The main changes we see as potentially impacting business are the 'right to switch off,' and unfair dismissal rights. We look at each of these in turn below.

Claims for Unfair Dismissal from Day 1

One of the major, and many would say the most significant changes under the Bill, is the introduction of rights for unfair dismissal from day one. Currently, employees need to have worked for a company for at least two years to bring an unfair dismissal claim. Considering the changes, we anticipate a potential rise in claims brought by employees. For this reason, employers should look to ensure probationary periods are included within the employee's specific contract of employment.

A 'right to switch off' from work

The Labour governments 'Plan to Work Pay' stated that "*We will bring in the right to switch off, so working from home does not become homes turning into 24/7 offices*".

Many employees often work additional hours outside of their standard contractual hours. However, the government's plans will give employees the right not to have to engage with work correspondence (including emails, telephone calls and instant messaging) outside of their contracted working hours. The government has stated that it will follow similar models / codes of practice to those already in place in certain countries across Europe. We don't envisage specific sanctions being introduced against employers. However, we do anticipate the need for employers to potentially change employees' contracts of employment to tailor them to the specific employee's role, and businesses needing to introduce a right to disconnect Policy.

It should be noted that there is no plan to bring in the right to bring a tribunal claim based solely on an employer's failure to follow the code of practice. However, workers who are repeatedly contacted outside of normal working hours may potentially be able to bring claims for constructive or unfair dismissal where they have been required to 'work' outside their stated contractual hours. To some extent employers can avoid potential claims with careful amendments to employees' current contracts of employment.

ESG, impact on Directors and Officer and Corporates

Environmental - Activist litigation

While activist litigation does not necessarily compel changes, it highlights public sentiment and such actions can be indicative that claims in a particular area, particularly in the Directors and Officers arena, are likely to increase in the coming years. In jurisdictions such as the Netherlands and England and Wales, there have been examples of derivative shareholder actions by non-governmental organisations seeking to compel net zero obligations, as opposed to claims for compensation or damages. Historically, climate litigation against companies was focused on the energy sector. However, greenwashing litigation is somewhat distinctive in that it is impacting a wide variety of sectors, from aviation to fashion.

In the Netherlands, the climate activist group Milieudefensie (or in English Environmental Defence) action against Shell was a groundbreaking decision which ordered Shell to reduce group-wide CO2 emissions of 45% by 2030. However, Shell appealed the ruling and on 14 November 2024 the Court of Appeal agreed that while Shell had an obligation to reduce its CO2 emissions, it disagreed with the lower court's imposition of a specific percentage by which emissions should be reduced.

The impact of climate change is also increasingly being felt in litigation in England and Wales against private companies. Although the 2023 derivative action brought by the activist group, ClientEarth, against the board of directors of Shell was unsuccessful, this is arguably at odds with a more general willingness on the part of the courts to entertain climate change and ESG-related actions.

All this means that businesses should remain diligent in actively reviewing and revising their internal climate policies. Boards must consider climate change and environmental protection within business strategy, paying attention to legislative developments, emerging regulations, and customer expectations. Pro-active engagement with these responsibilities will be essential to fending off the threat of climate litigation, as companies that fail to take adequate action may face legal challenges in the future from a range of stakeholder.

FCA Anti-greenwashing guidance

The FCA has been taking an increasingly proactive approach to ESG issues, and in particular, the risk that authorised entities may not be presenting a factually accurate picture of their own management of these risks, or the sustainability of their products, to the consumer. This includes the introduction of its finalised anti-greenwashing rules and guidance ("AGW"), which came into force on 31 May 2024.

All FCA regulated firms are in-scope, in respect of all products and services when they refer to the environmental or social characteristics of products or services, in any client communication to UK clients or financial promotion to UK persons. References to sustainability characteristics could be present in, but are not limited to, communications that include statements, assertions, strategies, targets, policies, information, and images relating to a product or service.

The FCA has stipulated that the anti-greenwashing rules require that Sustainability references should be:

1. Correct and capable of being substantiated
2. Clear and presented in a way that can be understood
3. Complete – they should not omit or hide important information and should consider the full life cycle of the product or service
4. Comparisons to other products or services are fair and meaningful

In developing the anti-greenwashing rules and guidance, those companies which make disclosures that are materially relied upon by investors and are found to be in breach of the regulations set out in the Financial Services and Markets Act 2023, FSMA may find themselves facing Section 90 and Section 90A claims – as referenced above.

Concluding comments

Whatever the outcome of 2025, it is imperative that all the data and knowledge at our fingertips is used to ensure that the best insurance cover is available to our customers in their time of need when an event does occur. Trend analysis and our lived claims experience can aid all parties in giving the correct coverage, and importantly to educate our customers in loss prevention and areas of potential exposure and risk. The best loss is the one that can be prevented before it even occurs.

As we said in the opening paragraphs of this article, and its importance cannot be overstated, a positive collaborative culture within an organisation is a risk manager's or insurance buyers most useful tool in their arsenal when it comes to tackling risk and claims mitigation.

January 2025

Contributors:

Laura Senior Claims Adjuster	Wall	Karey Senior Claims Adjuster	Pewtner
Annabel Senior Claims Adjuster/Solicitor	Philip	Zaheer Senior Claims Adjuster/Solicitor	Hashmi
Clare Senior Claims Adjuster/Solicitor	Munro	Andrew Senior Claims Adjuster/Solicitor	Cook
Robert Senior Claims Adjuster	Higgs	Gary Senior Claims Adjuster	Parlour
Sophie Senior Claims Adjuster/Solicitor	Halling	Rosie Team Leader – Major Loss/Solicitor	Wilson
Jack Senior Claims Adjuster/Solicitor	O'Neill		

COMHR315 (1/25) ZUR