trowers & hamlins

—— trowers.com

Regulations and resilience:

A roundup of fraud and cyber security developments in 2023

– Trowers & Hamlins – @trowers – @trowers_law

Contents

Introduction

2023 was a monumental year for the UK's fraud and cyber landscape. It is safe to say that AI well and truly embedded itself into our everyday lives, with legislative frameworks internationally attempting to keep up with the fast-paced developments, and its use becoming more prominent in cyber security – in both positive and negative ways. The National Cyber Security Centre (**NCSC**) has entered into its seventh year and continues to endeavour to make the UK the safest place to live and work online - whilst businesses build their cyber resilience, sophisticated cyber-attacks increase as threat actors use advances in technology to advance ransomware attacks and data breaches. Although we have seen great progress in areas of regulation in the EU and, to some extent, the UK, it is clear that 2024 will be a busy year for us and our clients in navigating developments.

As economic tensions continue so does financial crime and fraudulent activity. Whilst the UK Finance 2023 half year fraud update shows that figures fell by 2% in the first six months of 2023, with a total of £580million stolen, we are continuing to see a rise in advanced targeting via social engineering and AI. The targeting spans across individuals and companies alike, with finance and insurance remaining the most targeted industry sectors. It is of course not only the financial impact of fraud that is a concern, but the social and personal cost to victims. It is clear that the government's new Fraud Strategy, which intends to reduce fraud by 10% on 2019 levels by December 2024, is desperately needed. To that end, it is promising news to see the introduction of the Economic Crime and Corporate Transparency Act 2023, albeit now imposing an onus on businesses to ensure reasonable fraud prevention procedures are in place.

Before we embark on this year's journey of regulations and resilience, we look back on a handful of the key developments that the fraud and cyber security landscape has undergone in 2023.

Emily Sharples
Senior Associate
Dispute Resolution and Litigation
+44 (0)121 214 8874
ESharples@trowers.com

Amy-Rose Hayden
Associate
Dispute Resolution and Litigation
+44 (0)121 203 5672
AHayden@trowers.com

A roundup of key developments

Legislation

The Data Protection and Digital Information (No 2) Bill

The Data Protection and Digital Information (No 2) Bill (the **Bill**) progressed to committee stage in the House of Lords following the withdrawal of its predecessor and a replacement by Rishi Sunak's administration. The Bill intends to deliver on a number of issues including easing compliance on businesses and introducing safeguards to technologies, as well as updating digital verification, privacy and electronic communications regulations and modernising the Information Commissioner's Office (**ICO**).

As Viscount Camrose aptly summarised on 19 December 2023:

> **"In 2018 Parliament passed the Data Protection Act, which was the UK's implementation of the EU general data protection regulation. While the EU GDPR protected the privacy rights of individuals, there were unintended consequences. It resulted in high costs and a disproportionate compliance burden for small businesses. These reforms deliver on the Government's promise to use the opportunity afforded to us by leaving the European Union to create a new and improved UK data rights regime."**

At first blush the Bill would appear a welcome resolution to a great deal of the issues businesses and consumers are facing. The downside to the Bill encompassing such a broad variety of areas, however, is the need for a catch-all solution, which cannot keep up with the digital evolution fast enough. A number of new clauses have been introduced to the Bill, on which the ICO has been consulted. On 18 December 2023 the Commissioner's updated response (the original having been published in March 2023) was published on the ICO's website. The Commissioner expressed that he was pleased to note some changes in response to his comments, however the large majority remain unaddressed by the government and certain of the new clauses require wider public consultation. The Bill will progress through Parliament during 2024 and will have wide-ranging consequences for data protection legislation.

EU Data Act

In the EU, in November 2023, the European Council adopted the EU's Data Act (**Data Act**), which will apply from 2025. The Data Act aims to facilitate the sharing of data in order to assist both individuals and businesses in balancing data access and trade secret protection. This will mean that businesses will need to review their practices and policies to adhere to the new legislation, for example in updating their data management systems and contractual arrangements to Data Act standards. The Data Act, together with the UK-US commitment to establish a data bridge for the UK Extension to the EU-US Data Privacy Framework, which is set to offer more robust protection for the free flow of data between organisations in the UK and participating organisations in the US, demonstrates that the safe sharing of data and international cooperation will continue to be high on the agenda as we go into 2024.

Economic Crime and Corporate Transparency Act 2023

On 26 October 2023 the Economic Crime and Corporate Transparency Act 2023 (**ECCTA**) received royal assent and introduced in a new fraud offence. Similar to the corporate offences in the Bribery Act 2010 (in relation to bribery) and the Criminal Finances Act 2017 (in relation to the facilitation of tax evasion), ECCTA introduces a *failure to prevent fraud* offence which imposes criminal liability on certain corporate entities where they benefit from the fraudulent activities of "associated" persons.

Once in effect, a "large organisation" will be guilty of the new offence if a person "associated" with the organisation commits a fraud offence intending to (directly or indirectly) benefit either the organisation or any person or subsidiary undertaking that that the associated person provides services to on behalf of the organisation.

The definition of an "associate" is broad, and includes employees, agents, subsidiaries and those who otherwise perform services for or on behalf of the organisation.

The offence will only apply to large entities where at least two of the following apply:

- turnover of £36 million or more
- balance sheet assets of £18 million or more
- 250 or more employees

The organisation will not be guilty of the offence if it was, or was intended to be, a victim of the fraud offence. Additionally, it will be a defence if the organisation can prove that at the time the fraud offence was committed:

- it had reasonable fraud prevention procedures in place; or
- it was not reasonable to expect such prevention procedures to be in place

Although ECCTA is law, the failure to prevent fraud offence is not expected to come into force until Spring 2024. Given the defence available organisations should plan ahead and protect themselves by ensuring specific fraud prevention procedures are in place. If you require any assistance in implementing fraud or financial crime policies or reviewing existing policies to ensure compliance, please contact Elizabeth Mulley, Emily Sharples or Amy-Rose Hayden.

Guidance

The National Cyber Security Centre (**NCSC**) and the ICO remain active in enhancing the UK's cyber security standards. In September 2023 the two organisations signed a joint Memorandum of Understanding establishing a framework setting out six key areas in which the organisations will increase areas of collaboration including the development of cyber security standards, information sharing, incident management and public communications. Whilst no legally binding obligations have been created for either party, it seems to be a constructive step toward collating UK guidance and building a culture of cooperation in cyber security. We will be keeping a close eye on how this collaboration works moving forward into 2024.

NCSC

In its Annual Review for 2022-2023, the NCSC, the UK's technical cyber security authority, sets out that it issued 24.48 million notifications, informing organisations that they were experiencing a cyber incident, through its automated Early Warning service. Uptake in the NCSC's Cyber Essentials scheme continues with the number of Cyber Essentials certificates awarded in the past year increasing by 21% to 28,399 overall. NCSC states that 141,712 Cyber Essentials certificates in total have been awarded since the scheme began and its data suggests that 80% fewer cyber insurance claims are made when Cyber Essentials is in place.

NCSC publishes guidance on a wide range of topics from Cyber Essentials to cryptography to supply chain guidance. Supply chain attacks are an increasing threat to corporate cyber security and have been recognised as a growing risk by the Cyber Security Government Strategy 2022 – 2030. The NCSC reviewed their guidance on 12 October 2023 setting out key principles for business to establish control and oversight into their supply chain's cyber security.

In addition, ransomware remains one of the most prolific cyber threats in the UK, with cyber criminals stealing and encrypting data for a ransom to maximise profits. The NCSC, ICO and law enforcement continue to adopt their guidance from 2022 that they do not encourage nor condone the payment of ransom demands for several reasons, including:

- if you pay the ransom there is no guarantee you will be able to access the data
- you are more likely to be targeted in the future
- the potential civil and criminal implications of paying criminal groups

ICO

The ICO is the UK's independent regulator, continuing to assist in upholding data privacy rights for individuals, as well as noting AI as a priority area due to the potential risks to individuals and their rights and freedoms. In particular, the ICO has set out its current areas of focus in AI:

- fairness
- dark patterns
- AI-as-a-service
- AI and recommender systems
- biometric data and technologies
- privacy and confidentiality in explainable AI

The ICO has published guidance and practical resources including, in April 2023, its list of eight questions that developers and users need to ask when developing or using generative AI that processes personal data as well as its AI and data protection risk toolkit to encourage the safe adoption of AI across sectors.

In the absence of AI regulation / legislation in the UK, the ICO together with existing data protection laws remain the only recourse in the AI sphere, as explained in more detail below. For example, in October 2023 the Information Commissioner issued a preliminary enforcement notice against Snap, Inc and Snap Group Limited (**Snap**) due to the provisional findings of their investigation into privacy risks posed by its generative AI chatbot 'My AI' which "*suggest a worrying failure by Snap to adequately identify and assess the privacy risks to children and other users…"*.

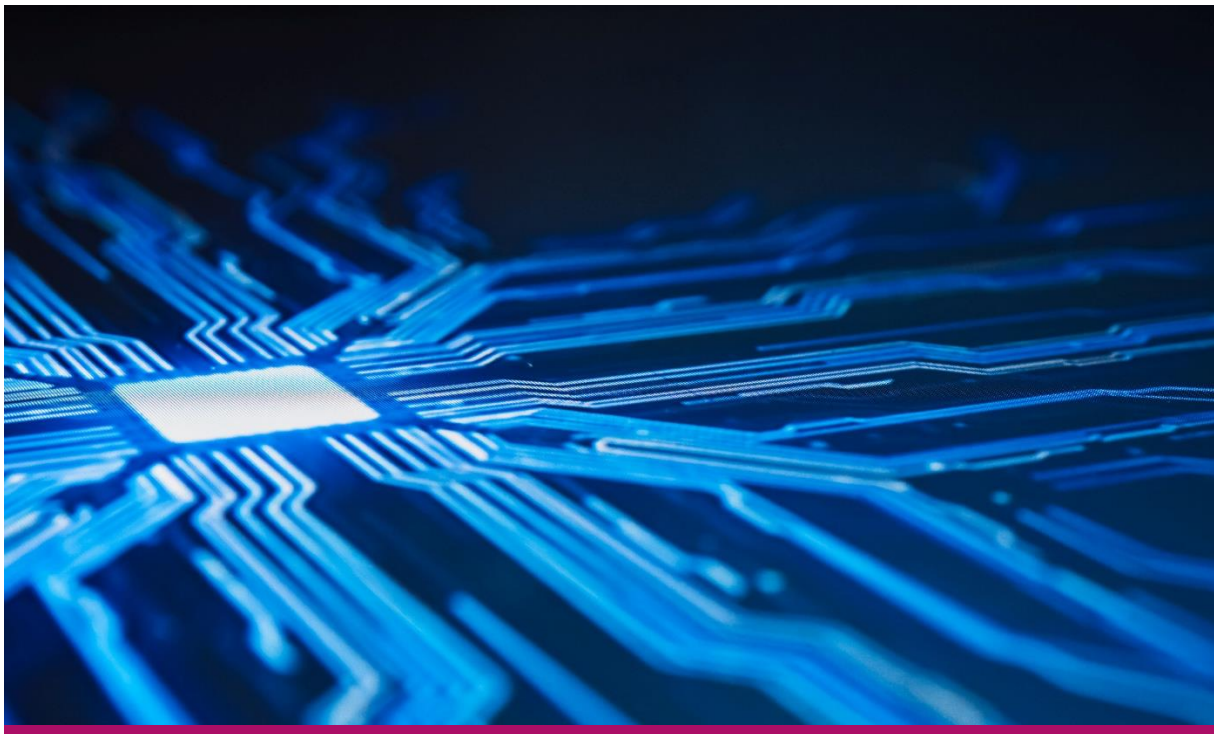
Artificial Intelligence

Whilst the UK has not enacted any specific binding legislation, it is currently relying on existing legislation, including the Equality Act 2010, and Data Protection Act 2018 (**DPA 2018**) etc., to regulate use of AI, and focusing on providing guidance and best practices for industry as opposed to prescriptive rules. The government has published a white paper outlining its approach to AI regulation, advocating a pro-innovation approach. The white paper seeks to create an environment which allows the UK to be at the forefront of technological developments. Instead of regulation, the UK's approach aims to encourage competition and enhance public trust, however the current lack of regulation in the UK could result in less protection and greater risks for businesses and users alike.

In contrast, the EU has taken a more comprehensive and risk-based approach to AI regulation, with the proposed EU AI Act being the centrepiece of its regulatory efforts. The EU AI Act, having been in discussion for over a decade, aims to establish a framework for the development, deployment, and use of AI systems in the EU, with a focus on protecting fundamental rights, safety, and fairness. The EU AI Act will establish obligations for both providers and users

depending on the level of risk from AI – assessing the level of risk posed by a system. For example systems deemed an unacceptable risk will be banned, such as cognitive behavioural manipulation of people or social scoring (classifying people based on socio-economic status, behaviour or personal characteristics). See our AI: Threat or Opportunity insight report here for more detail on this.

The UK hosted the first ever global AI Safety Summit (the **Summit**) on 1 and 2 November 2023. The Summit was attended by international governments, executives leading AI companies, civil society figures and expert researchers to consider the key risks of AI systems, goals for mitigating these risks and improvements in AI safety. A series of significant commitments were made at the Summit - perhaps the most significant of which being the Bletchley Declaration, the world-first agreement on the safety of AI. The Bletchley Declaration had signatories included 28 countries, including those that are at the forefront of developing AI technologies such as the UK, US, China, the EU and Japan. The Bletchley Declaration identified risks anticipated with AI systems such as misuse, cybersecurity, disinformation, biotechnology, privacy concerns, and ability for bias. It will focus on building risk-based policies internationally. With the next Summit in May 2024, AI will continue to be an area of fast-paced change that businesses and users alike will need to keep up to date with.



Case law - Fraud

Authorised Push Payment Fraud

Fiona Philipp v Barclays Bank UK PLC [2023] UKSC 25

In July 2023, the Supreme Court handed down its landmark decision on the scope of a bank's duties in circumstances where a customer is the victim of an authorised push payment (**APP**) fraud.

Mrs Philipp issued proceedings against Barclays after a sophisticated APP fraud resulted in her and her husband transferring the majority of their life savings to a fraudulent third party. Mrs Philipp sought to argue that Barclays had breached its contractual and/or common law duty of care to exercise reasonable diligence and care in circumstances where it had reasonable grounds for believing a fraud was occurring.

The Supreme Court, however, held that a bank cannot be liable where clear instructions are given by a customer (either an individual or an agent with apparent authority) on which the bank was obliged to act even if such instructions were procured by fraud. As the banks breath a huge sigh of relief, this decision ensures the onus remains on customers to avoid the fraudulent scams which increase in number and sophistication year on year.

An in-depth look at the facts of the case, its procedural history and the Supreme Court decision can be found in an article written by Emily Sharples here.

Fraud and Limitation

Seedo v El Gamal and others [2023] EWCA Civ 330

2023 also saw the Court of Appeal consider the application of section 32(1)(a) of the Limitation Act 1980 and provide some useful guidance on limitation in fraud cases. In a claim brought against a solicitor for fraudulent misrepresentation and breach of retainer in relation to a property investment, the Court of Appeal held:

1. **Timing**: If a limitation defence is dealt with at trial, and following a determination of the facts, the Court should base its decision on the date its finds that the Claimant discovered (or should reasonably have discovered) the fraud. Whereas, if limitation is decided as part of an interim application, the decision must be confined to the case as pleased (as no findings of fact have yet been made).

2. **Multiple Lies**: If a Claimant is deceived by more than one lie, a new limitation period will only start to run if a later lie gives rise to a different cause of action – i.e. a later lie will not start a new clock running if the dishonesty is connected and part of the same overall deceit.

In *Seedo*, the Defendant solicitor's lies were connected and could not be considered as separate acts of deceit giving rise to multiples causes of action. The period for limitation therefore commenced from the earlier date, when the Claimant first became aware of the fraud.

Fraudulent Trading, S. 213 Insolvency Act 1986

Tradition Financial Services Ltd v Bilta (UK) Ltd [2023] EWCA Civ 112

In another key case in 2023, the scope of Section 213 of the Insolvency Act 1986 ("**IA**") was considered by the Court of Appeal.

The proceedings arose out of a "MTIC" fraud[1] relating to spot trading in carbon credits dating back to 2009. The Claimants, who became insolvent due to significant VAT liabilities, issued proceedings (by their liquidators) against various Defendants, including Tradition. One of the causes of action advanced was that Tradition, by its directors, had participated in the fraudulent trading of the Claimants' businesses pursuant to S. 213 IA.

Section 213 (2) IA states:

> **The court, on the application of the liquidator may declare that any persons who were knowingly parties to the carrying on of the business in the manner above-mentioned are to be liable to make such contributions (if any) to the company's assets as the court thinks proper.**

Tradition sought to argue that S. 213 should be restricted to those persons exercising management or control of the entity in question. However, the Claimants relied on the literal interpretation of the provision, arguing that any person who was aware of the fraudulent dealings of a company, was a "party to" the fraudulent carrying on of that business.

The Court held that in the circumstances, S. 213 should be interpreted more widely, in order to include an "outsider" who had been party to the carrying on of the business. Whilst there was no binding authority on whether S. 213 applied to a person or entity who was not directly party to the fraudulent activity, the Court found that the wider interpretation was more aligned to the purpose of S. 213 (i.e. to make those who had been party to fraudulent trading liable to compensate the creditors of the fraudulent company). However, Lord Justice Lewison highlighted that the matter is fact specific and his judgment was not intended to set an outer limit for the scope of S. 213 IA.

Legal Professional Privilege and the Iniquity Exception

Enigma Diagnostics Ltd v Boulter [2023] EWHC 1999 (Ch)

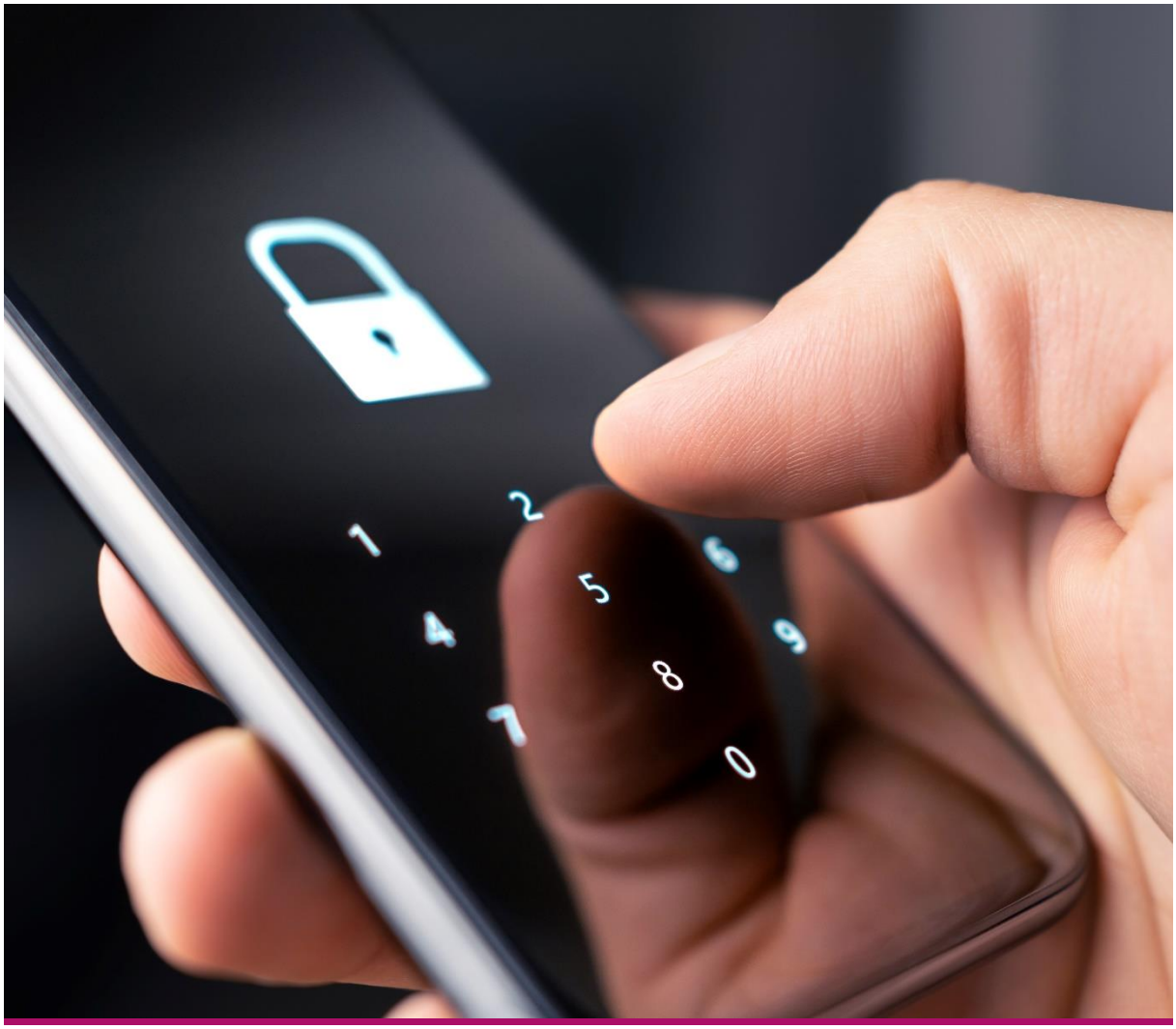
Although only a High Court ruling, this case featured the rarely applied iniquity exception in arguments of legal professional privilege.

The matter related to the Defendant's dealings in shares of the Claimant company (such dealings the Claimant alleged to be fraudulent). Proceedings were also brought against DLA Piper UK LLP (**DLA**) and the individual solicitor for their involvement in the share arrangements which formed the basis of the claims.

[1] Missing trader inter-community fraud.

By way of an interim application, the Claimant sought disclosure and inspection from DLA and the solicitor, who were the only parties who had retained substantial contemporaneous documents. DLA disputed the application and sought to withhold production of documents on the basis of legal advice privilege. The Claimant, however, argued that the iniquity exception to privilege applied – on the basis that there is no privilege in documents which themselves are part of the fraud (*R v Cox & Railton* [1884] 14 QBS 153).

The Court ruled in the Claimant's favour, holding that privilege does not attach to documents where the solicitor was instructed for the purposes of furthering the fraud (albeit the solicitor may not have been aware of the purpose).



Case law – cyber

As the Courts come across more cases linked to AI, December 2023 saw a landmark ruling by the Supreme Court that an AI machine cannot be called an inventor of new products or ideas in *Thaler v Comptroller-General of Patents, Designs and Trademarks* [2023] UKSC 49. We have also witnessed some cautionary tales for those seeking to use AI without checking its output – for example in respect of submissions to Court, such as in *Harber v Commissioners for His Majesty's Revenue and Customs* [2023] UKFTT 1007 (TC) whereby unfortunately Mrs Harber provided case law that did not exist produced by an AI system.

In terms of data privacy and confidential information claims, these remain frequently before the Courts. We have summarised a number of noteworthy decisions relating to these topics from 2023:

- *R (on the application of Delo) v Information Commissioner [2023] EWCA Civ 1141* – in a unanimous decision, the Court of Appeal set out the parameters of the ICO's duties regarding complaint handling. The Court determined the responsibilities of the Information Commissioner (operating through the ICO) when a data subject lodges a complaint alleging that a data controller has infringed data protection law; holding that the ICO has a discretion as to whether or not to investigate a complaint regarding a data controller. Further, the ICO's discretion is to be exercised in a reasonable and proportionate manner. For example in some cases it may be appropriate to take an alternative course of action such as the provision of advice and guidance.

- *Armstrong Watson LLP v Persons unknown [2023] EWHC 762 (KB)* – Armstrong Watson successfully applied without notice for an interim injunction to prohibit the unidentified cyber criminals from disclosing or communicating information stolen in a ransomware attack. In this case the Court provides a helpful summary of criteria to be applied when considering injunctive relief (applying the American Cyanamid principles) and the competing rights that the Court will take into account, as well as the practical considerations when seeking an injunction against 'persons unknown' following a cyber-attack including service.

- *Österreichische Post (Préjudice moral lié au traitement de données personnelles) Case C-300/21* – the Court of Justice held that mere infringement of Regulation (EU) 2016/679, the EU General Data Protection Regulation (EU GDPR) does not give rise to a right to compensation, however there is no requirement for the non-material damage suffered to reach a threshold of seriousness before compensation can be claimed. For instance, suffering upset should not be dismissed as not being sufficiently serious. In order to claim compensation, however, an infringement and actual damage, together a causal link between the two, must be evidenced. The amount of compensation is then determined under national rules of each Member State provided they do not hinder the exercise of rights under the EU GDPR. Whilst the Courts in England and Wales are not bound by this decision, they are free to have regard to it.

- *Ali v Chief Constable of Bedfordshire Police [2023] EWHC 938 (KB)* – this case analyses whether disclosure (of all or part) of the information was necessary to be included in a safeguarding referral to a local authority, and whether Ms Ali had a reasonable expectation

of privacy in the information. Ms Ali brough claims for breach of the UK GDPR, misuse of private information, breach of confidence and breach of her right to respect for private and family life derived from Article 8 of the European Convention on Human Rights **(ECHR)**. The Court held that in fact the disclosure had not been necessary, and Ms Ali's claims succeeded, with damages awarded. The judgment of Mr Justice Chamberlain helpfully culminates a number of determinations found in existing case law into one authority, see our article here.

- *X v The Transcription Agency LLP and another [2023] EWHC 1092 (KB)* – in what is understood to be the first High Court decision on this issue, the Court determined a broad construction was applicable under the United Kingdom General Data Protection Regulation, Retained Regulation (EU) 2016/679 **(UK GDPR)** under the DPA 2018 when 'acting in a judicial capacity' or if disclosure would likely prejudice judicial independence (the judicial exemption). The Court held that judges and third parties (such as court transcribers to the extent that they may be controllers of the information) may benefit from the judicial exemption in a wider range of circumstances than internal guidance had previously envisaged, and that the scheme for access to personal data is not to be used as a way to avoid the limits of appellate jurisdiction.

Get in touch

Trowers & Hamlins works with its clients together with our trusted partners, such as cyber security companies and funders, in ensuring their businesses have assessed and accounted for the above risks as well as supporting them through the aftermath of when a fraudulent incident is discovered.

Please do not hesitate to contact the writers of this article should you have any queries on the implications of the Report on your organisation or want to know more about how we can help stress-test and improve your businesses' armoury.

Helen Briant
Partner
Dispute Resolution and Litigation
+44 (0)121 214 8867
HBriant@trowers.com

Charlotte Clayson
Partner
Dispute Resolution and Litigation
+44 (0)20 7423 8087
CClayson@trowers.com

Jamie De Souza
Partner
Dispute Resolution and Litigation
+44 (0)121 214 8847
JDeSouza@trowers.com

Elizabeth Mulley
Managing Associate
Dispute Resolution and Litigation
+44 (0)121 214 8864
EMulley@trowers.com

Emily Sharples
Senior Associate
Dispute Resolution and Litigation
+44 (0)121 214 8874
ESharples@trowers.com

Amy-Rose Hayden
Associate
Dispute Resolution and Litigation
+44 (0)121 203 5672
AHayden@trowers.com