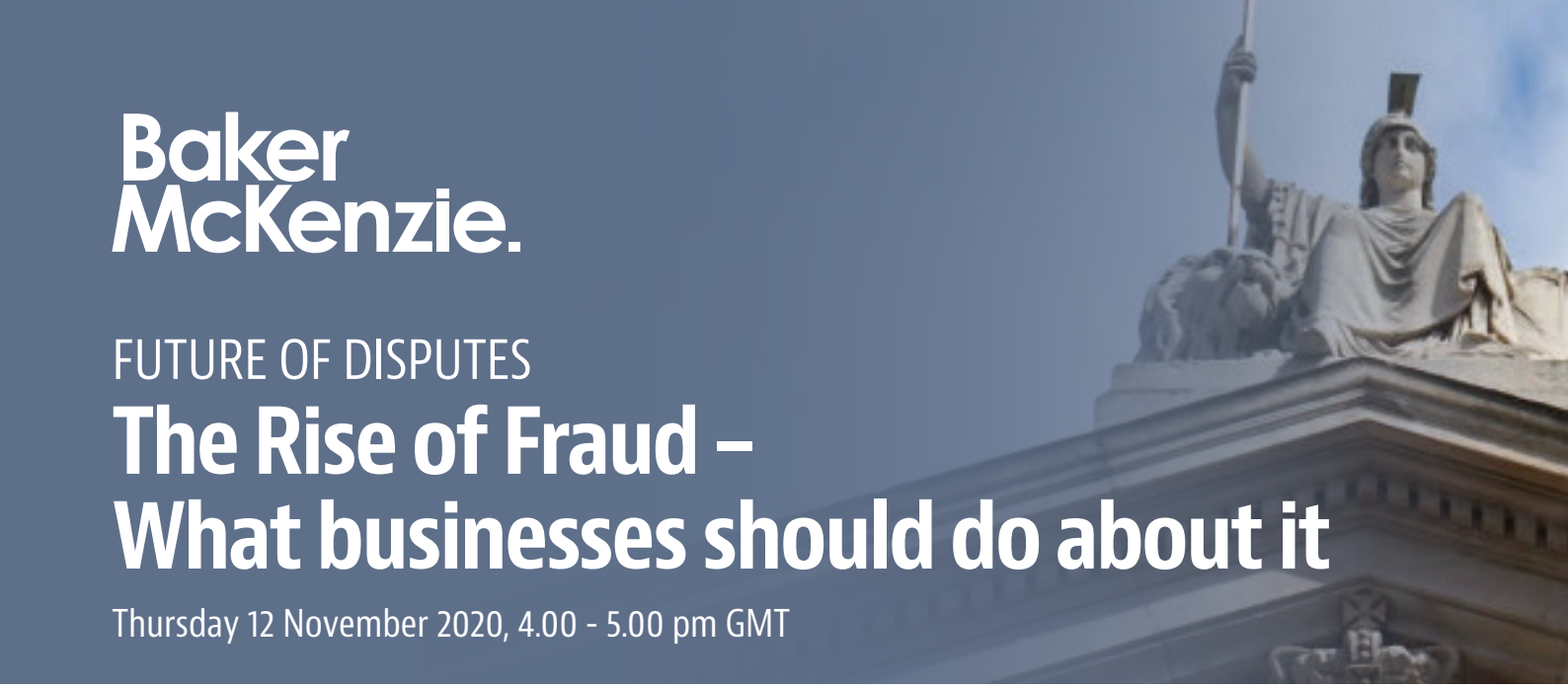

Baker McKenzie.

FUTURE OF DISPUTES

The Rise of Fraud – What businesses should do about it

Thursday 12 November 2020, 4.00 - 5.00 pm GMT

Key Takeaways...

from Baker McKenzie's Future of Disputes spotlight session

Fraud on the rise

Almost half of the respondents to a recent PwC survey reported having experienced fraud in the past 24 months[1], being the second highest reported incidence in 20 years. This trend is only likely to continue as a result of the COVID-19 pandemic.

Hard economic times always lead to a rise in fraud. First, it may be seen as a way to cover up poor performance and to "make ends meet". Second, fraud that has already taken place is often uncovered during difficult financial periods; as Warren Buffett put it, "only when the tide goes out do you discover who has been swimming naked".

COVID-19 also brings with it new opportunities for fraud: (a) a workforce working from home, (b) faced with the challenge of keeping hard-copy documents confidential, (c) using technology not designed to be used away from the office, and (d) increasingly using informal modes of technology to communicate with clients and customers (e.g. WhatsApp); coupled with (e) decreasing physical supervision and (f) the associated reduction in visibility by supervisors and management.

Cybercrime in the spotlight

Technological advances are only likely to increase the prevalence of cybercrime, and open new opportunities for fraudsters. The ever-increasing complexity of IT systems and the data supply and management chains mean that attack surfaces are growing fast. Now, not only does ransomware encrypt data (such that companies may decide to pay to 'release' their data), it also downloads the data in the background (such that the stolen IP or personal data may be sold for a profit). Similarly, in the context of payment diversion frauds, attacks that are currently the preserve of the technologically advanced criminal will rapidly become more commonplace. For example, we have already seen the use of "deepfake" audio, mimicking the voices of senior management and directing employees to divert payments away for the true recipients to line the pockets of fraudsters.

In cybercrime – as with many types of fraud – prevention and preparation are more cost-effective than cure. There are a number of precautionary steps that can and should be taken by businesses to protect and mitigate against the increasing risks of online fraud and cybercrime.

- **Understand the likely impact on the business.** For example, what is the delta between live and backed up data? How quickly can the data be restored? Understanding in advance the potential impact on the business will enable you to make informed and decisive decisions in the middle of a crisis.
- **Know your risk areas.** Audit and understand your data supply and management chain; not just third parties, but fourth, fifth and sixth parties as well.
- **Plan for cyber incidents.** Build a team of first responders (and back up in case those people are unavailable) and give people defined roles. Know who your external forensic experts and specialist legal counsel are in advance, and integrate them into your response processes.
- **Prepare and test response processes, both internally and alongside external advisors.** Conduct a post-mortem after the exercise to examine what did and did not work, and change things as necessary.
- **Engage with law enforcement when appropriate.** In certain circumstances, law enforcement assistance can be invaluable, so make use of that resource.

[1] PWC's 2020 Global Economic Crime and Fraud Survey found that almost half (47%) of the 5000+ respondents had experienced fraud in the past 24 months.

Public policy developments ahead

The future of the Serious Fraud Office (SFO) as the specialist prosecuting authority tackling serious and complex crime remains uncertain. It was proposed that the SFO should be subsumed into a larger, multi-disciplinary agency under the control of an expanded National Crime Agency. While it has disappeared from the immediate legislative agenda (giving way to other priorities, such as Brexit), the debate may resurface in light of recent high profile cases which have cast further doubt on the SFO and public spending considerations. A merger would develop an intelligence-led approach to the investigation and prosecution of serious and organised crime, a single set of consistent standards between constituent parts of the investigation and prosecution process, and associated financial efficiencies.

The doctrine of attribution and the "identification principle" results in difficulties for courts and juries establishing that senior individuals comprise a company's directing mind and will. Recent decisions have confirmed that boards and board sub-committees are the directing mind and will of a company, not the executive management that serves up opportunities for execution at the board's direction. This does not provide for the reality of multi-national companies, and the UK Government has called for reform to ensure that the UK does not fall behind international standards in the prosecution of economic crime. The Law Commission – led by the Commissioner for Criminal Law and the Commissioner for Commercial and Common Law – is aiming to publish an Options Paper by late 2021. One such "Option" is likely to be an extension of the law to create a strict liability 'failure to prevent economic crime' corporate offence (akin to the "failure to prevent bribery" offence under the Bribery Act 2010 and the more recent "failure to prevent the facilitation of tax evasion" offence under the Criminal Finances Act 2017).

Policy reform, coupled with the increasingly flexible approach taken by the English Courts (for example, granting injunctions against "persons unknown", or allowing service of proceedings electronically by Facebook or WhatsApp) will support the focus on positioning the English legal system at the forefront of the fight against fraud.

If you would like any more information, please contact us:

Kate Geale
Associate,
Dispute Resolution
kate.geale
@bakermckenzie.com

Paul Glass
Partner, Data Protection
and Cyber Security
paul.glass
@bakermckenzie.com

Jonathan Peddie
Partner,
Dispute Resolution
jonathan.peddie
@bakermckenzie.com

Hugh Lyons
Partner,
Dispute Resolution
hugh.lyons
@bakermckenzie.com

Charles Thomson
Partner,
Dispute Resolution
charles.thomson
@bakermckenzie.com

bakermckenzie.com