Fraud Prevention and Response Hub

大成 DENTONS

Overview

Fraud has become one of the most prevalent threats facing both individuals and businesses today. As technology develops, so do the ways in which fraudsters target their victims. These can range from complex instances of cybercrime to relatively simple authorised push payment or phishing scams.

We have developed this site to provide you with practical advice and assistance in preventing and responding to fraud.

Businesses

For businesses, it is crucial to develop and maintain adequate fraud policies. This includes having in place internal monitoring and reporting mechanisms, insider threat policies and cybercrime detection systems. If fraud does occur, businesses must be ready to react quickly and efficiently. As payments become quicker and easier, fraudsters are able to move money between countries in a matter of moments. Businesses will often need to take a multi-jurisdictional approach to ensure that they take appropriate legal action to freeze and recover funds. It is important to have a response plan in place to ensure that help is swiftly sought and losses are mitigated.

Financial institutions

The picture becomes even more complex when considering fraud from the perspective of financial institutions. Following, the *Which?* super-complaint, it became clear that there is an increasing appetite to hold banks and other financial institutions responsible in cases where their customers have fallen victim to fraud. Financial institutions are expected to take adequate steps to protect their customers from fraud. The nature of this obligation has been considered and clarified by the courts in recent case law, which includes decisions on the scope of the *Quincecare* duty of care.

The desire to make payments safer has prompted an increased focus on ongoing monitoring of payment mechanisms, including the development of the Confirmation of Payee model.

Similarly, there is an increased pressure on financial institutions to compensate victims of fraud. Following a consultation period, a number of banks have signed up to the Contingent Reimbursement Model Code for Authorised Push Payment Scams. This Code obliges banks to compensate victims of push payment fraud, even if they are not at fault, and victims are able to enforce these obligations by raising a dispute with the Financial Ombudsman Service. Although limited in application, the Code is likely to become best practice in the sector.

The desire to fight APP scams and assist victims is no doubt a positive development. The Code is, however, likely to raise a number of complex legal questions and may result in legal challenges. Some of these are considered in the Insights section as well as in this document.

You may also find our Global Injunctions Toolkit helpful.

Your Key Contacts

United Kingdom

Daren Allen
Partner, London
D +44 20 7246 7651
M +44 7515 919812
daren.allen@dentons.com

Marija Bračković
Senior Associate, London
D +44 20 7246 7485
M +44 79 2050 4734
marija.brackovic@dentons.com

Craig Neilson
Partner, London
D +44 33 0222 1912
craig.neilson@dentons.com