CLIFFORD
CHANCE

THE GROWING RISK OF GROUP LITIGATION AND CLASS ACTIONS

— THOUGHT LEADERSHIP

APRIL 2022

THE GROWING RISK OF GROUP LITIGATION AND CLASS ACTIONS

Class actions have long been a feature of the legal landscape in the US, but there are clear indications that their reach is expanding. In this extract from a recent webinar, Clifford Chance experts explore the key risks in relation to securities and shareholder litigation, claims arising from data breaches and data misuse, and climate change litigation.

"Class or group actions have become a regular feature of American corporate life, driven by generous class mechanisms, the absence of a "loser pays" rule and contingency fee lawyers," says Ian Moulding, a Clifford Chance litigation Partner based in London. "Now mass claims are on the rise in many countries, fueled by proactive, entrepreneurial claimant lawyers, a generally more litigious environment and the explosive growth in the availability of third-party funding options and the related costs insurance."

In the UK, for example, very significant group actions have been filed across a range of sectors, including: the RBS Rights Issue litigation and the Lloyds/HBOS claims following the GFC in the financial sector; the VW diesel emissions action in the consumer sector; the Tesco accounting error shareholder action; the Google iPhone litigation with respect to data privacy; and a raft of competition-related claims, including the Mastercard fees litigation and the FX market group actions. Environmental claims, such as the CO2 emissions litigation brought by a group of NGOs against Shell in the Netherlands, is another fast-developing area.

Crucial to these actions is the backing of litigation funders, which is now a multi-billion dollar international business. Around three quarters of such claims in the UK are funded, as Moulding explains: "One area which is attracting funders in particular is shareholder securities claims, or "stock drop" cases as they are known in the US. In the UK, these claims are brought under sections 90 and 90A of the Financial Services and Markets Act (FSMA). They provide, respectively, a cause of action for untrue or misleading statements, or omissions in a prospectus or other listing particulars or in a company's annual reports and accounts."

The "Securities fraud" phenomenon

A number of claims in the pipeline in the UK follow the US model of stock drop claims. The pattern is as follows: some bad news emerges of wrongdoing (perhaps following a settlement with a government agency, or a DPA). There is a fall in the company's share price. Then a group shareholder action begins, alleging that the company failed to disclose the risk of the wrongdoing in a Prospectus or an Offering Document (for claims under s90 of FSMA) or in its report and accounts or other regulatory announcements (for claims under s90A of FSMA).

"The challenge for shareholder claimants is making a link between the wrongdoing that led to the share price fall and the company's earlier disclosure to the market. Because to be liable, it is not enough that the company was guilty of some wrongdoing that led to a share price fall, the company must have made an untrue or misleading statement in its financial statements, regulatory announcements or listing particulars," says Kelwin Nicholls, a London-based litigation Partner.

Claimants' lawyers work backwards, with hindsight, trying to identify statements that conflict in some way with the misconduct that led to the share price fall. And in undertaking this exercise, claimant lawyers quite often focus in on generic language that most companies include in their report and accounts about being good corporate citizens – "we comply with applicable laws, we act with integrity, our customers are important to us, etc."

In the US, Bloomberg journalist Matt Levine coined a term to describe this phenomenon – "everything is securities fraud". As he put it: "*A company does something bad, or something bad happens to it. Its stock price goes down, because of the bad thing. Shareholders sue: Doing the bad thing and not immediately telling shareholders about it, the shareholders say, is securities fraud. … And so contributing to global warming is securities fraud, and sexual harassment by executives is securities fraud, and customer data breaches are securities fraud. Anything bad that is done by or happens to a public company is securities fraud.*" *(Money Stuff, 6/26/19)*

Nicholls says "This a problem, because this approach to securities litigation effectively provides a two-way bet for shareholders. If the company gets away with misconduct, usually its shareholders gain through profits. And if the company gets caught and punished, shareholders win through securities litigation. The winners are shareholders who bring the claims – typically former shareholders who held shares when the bad thing happened. The losers are the company's current shareholders – they ultimately bear those costs and losses of these claims.".

There are two legal mechanisms to keep this trend in check. Both of them operated in a decision last year of the US Supreme Court in *Goldman Sachs v Arkansas Teacher Retirement System*. One mechanism is reliance – should claimants/plaintiffs have to prove that they relied on the specific statement they identify as being wrong, or is it sufficient that the market was generally misled (the so-called "fraud on the market" theory)? And secondly, can defendants challenge these claims on the basis that generic statements are too vague to give rise to liability?

The US Supreme Court decided in that case that defendants can argue at an early stage that the statements relied upon are too generic to support a claim. As to fraud on the market, the US Supreme Court decided that defendants bear the burden of displacing the fraud on the market theory of reliance, so that issue landed in favour of plaintiffs.

"It will be very interesting to see how the English courts come out on these two issues – whether generic statements of corporate policy are actionable under FSMA and how far claimants must go to establish causation and reliance, because without some controls around that, everything will become securities fraud in the English courts. We are certainly seeing echoes of that phenomenon emerging in the London shareholder claims market and this will affect claims based on a wide range of issues – climate change claims, data claims, me-too-style misconduct claims and so on, because this approach expands the pool of potential claimants from those who suffer the primary losses when these events occur (local communities, data subjects, consumers, employees, etc.) to cover the company's shareholders as well," says Nicholls.

How might this play out in the English courts?

It is likely that, for claims under s90A of FSMA, English courts will require claimants to prove reliance, and that will be difficult for them to do if they say they relied on very generic corporate statements of the kind that pretty much every company makes. We have seen in a procedural hearing in the Tesco group shareholder litigation, which settled before trial, that the High Court expected claimants to provide evidence of reliance.

Reliance is an ingredient of liability in s90A – the legislation says compensation must be paid to those who bought, held or sold shares *in reliance* on the company's published information. That raises a whole host of questions. Reliance by whom? Who within the shareholder needs to have relied on the relevant information? How does reliance work where you have index funds, such as a FTSE tracker, or a sectoral index fund? Reliance when? What if the company publishes its report and accounts this month, discovers a problem six months from now, and it becomes public next year? What degree of reliance? Does the claimant need to have read the actual statement it subsequently identifies as misleading, or is it enough that they reviewed the financial statements briefly? What if they didn't read them at all?

What degree of reliance? Does the claimant need to have read the actual statement it subsequently identifies as misleading, or is it enough that they reviewed the financial statements briefly? What if they didn't read them at all?

In s90 claims, the legislation doesn't use the word reliance. S90 relates to false or misleading statements in listing particulars, prospectuses, offering documents, etc. "Why should they be different from claims based on regulatory disclosures and financial statements? Probably because listing particulars are, for want of a better term, "selling documents". Reports and accounts and general regulatory disclosures are not. So, there is a logic to requiring claimants to prove reliance on general regulatory disclosures, but not for misstatements or omissions in "selling documents" like listing particulars," says Nicholls.

And he adds: "Does that mean that it is open season for claimants on s90 claims? No, I don't think it is, because s90 requires claimants to prove that they suffered a loss as a result of untrue or misleading statements, or omissions. If a prospectus says that "*integrity and honesty are at the heart of our business*", and it turns out someone in their organisation has been guilty of dishonesty somewhere in their global operations, has the claimant suffered a loss as a result of an untrue or misleading statement? I would be surprised if it turns out to be that easy for claimants in the English courts."

A rise in claims for data breach

Data class actions are a growing risk for businesses, on two fronts. First, serious data breaches (such as ransomware incidents) can give rise to shareholder claims. In 2017, Yahoo was one of the first companies to be sued by shareholders in the US who alleged that Yahoo's public filings identifying robust data security systems and processes were inaccurate, following significant data breaches in 2015 and 2017. Yahoo ultimately settled the litigation for USD 80 million. All companies hold significant volumes of personal data relating to individuals – whether that's just the personal data of their employees or, for many businesses, the personal data of customers too. That is protected under data privacy regimes, such as the GDPR in the UK and EU, and similar privacy regimes globally. Beyond personal data, firms may hold client or transactional data, which may be confidential. So, when that data has been exfiltrated in a data breach, customers look to the company for damages. That gives rise to a second risk, of data claims against the company.

Procedurally, under English law, data claims take the form of actions for breach of statutory duty, breach of confidence or misuse of private information, or even straightforward breach of contract or negligence claims. "Perhaps the most significant exposures stem from cyber incidents impacting thousands or millions of customers or clients," says London-based, Clifford Chance litigation Partner, Kate Scott.

In the English courts, we have seen claims following cyber incidents issued against British Airways, Marriott, and Equifax (amongst others) – driven by litigation funders and claimant firms seeking to build a book of claims. "What's interesting, is that to date in the English courts, we've not yet seen claims, like the British Airways claims get to trial, with many claims being settled at an early stage," says Scott. "Why is that? Often claims are managed under a Group Litigation Order – a procedural mechanism allowing claims that give rise to common or related issues to be managed together. But this is an opt in mechanism – i.e. claimant firms had to identify actual claimants, willing to enforce their data rights. And in reality, it can be hard to persuade claimants to take action. Whilst many are concerned about their data privacy rights, in a world where it isn't yet clear that a breach of those rights leads to significant compensation, many consumers need to be persuaded to act, particularly where companies organise identity theft protection. But, I think we are seeing a shift on that issue driven by increasing awareness of those issues and privacy organisations," she says.

Companies like British Airways raise a variety of plausible defences to the claims, including:

- That it is for the claimants to show that the company failed to demonstrate compliance with GDPR.
- That much of the personal data compromised was largely in the public domain, was not confidential, or was not such to create a reasonable expectation of privacy.

Our briefing here, explores the defences to data claims in more detail.

There has recently been a helpful decision in *Warren v DSG* Retail (which operates the Currys PC World and Dixons Travel brands). It was the victim of a cyber incident, during which the attackers accessed the personal data of DSG's customers. The Claimant alleged that certain personal information – his name, address, phone number, date of birth and email address – was compromised in the attack. In a summary judgment application, the English court agreed with DSG that for a breach of confidence, there must be some positive wrongful action in relation to the Claimant's information, and held that no duty of care was owed by DSG to the Claimant. So, those claims will not proceed to trial. "The decision did not impact the statutory DPA claims – those remain to be determined. So, watch this space. Notwithstanding the difficulties, I think we will continue to see a steady flow of claims being issued after cyber attacks. Board members need to appreciate the data litigation risk when the company is handling a serious incident," Scott adds.

Data misuse class actions

These are often claims where personal data has been processed for one purpose, but wrongly used for another. The core issues here might be issues of consent. It might be because other requirements of GDPR have not been met – e.g. in relation to automated processing. It might be because data has been scraped.

Perhaps the best example of this in the English courts is the *Lloyd v Google* action, and the Supreme Court judgment that was handed down last year. The case concerned Google's use of cookies to harvest browser-generated data to sell to advertisers, without the consent of iPhone users. But the significance of the case is in its test of the representative procedure in the English courts. Representative claims may be brought by or against one or more persons who have the "same interest" in the claim; and are brought on an "opt-out" basis – the represented class does not need to be joined as parties to the action. "Opt-out" claims identify the class, and do not rely on individual data subjects opting in to the claim (as is the case with the GLO process).

"That's why representative actions are so attractive to litigation funders: it is because they increase the claim size – in *Lloyd v Google* an individual claim would below value, but there are millions of data subjects – in this case, four million iPhone users. In *Lloyd v Google*, any losses based on individual circumstances were disavowed, arguing that each iPhone user suffered the same damage and should get the same sum in compensation – damages for loss of control of data. No distress or other loss arising from the breach was pleaded," explains Scott.

Where the extent of the damage suffered was not the same for each claimant (as in the case of the iPhone users) and an individualised assessment is required, representative actions are unlikely to work. The Supreme Court left open the point that they may, in theory, be brought as part of a bifurcated two-stage process, that is unlikely to be economically attractive for claimants and litigation funders.

The other central issue in *Lloyd v Google* was whether the claimants could obtain damages for loss of control of data alone. The Supreme Court said no: In order to assess compensation, it is necessary to prove what unlawful processing of personal data relating to a given individual occurred, which requires in many cases considerable factual analysis. Although the judgment addresses the position under the UK Data Protection Act 1998, which predates the GDPR, Scott considers that it is unlikely that a different result would be reached under GDPR as applied in England.

"What does that mean in terms of trends? I think we are going to see claimant firms and litigation funders focus on claims where there is the potential for more significant damages awards and the potential returns are higher," Scott says.

Areas of focus include the use of artificial intelligence to process personal data, with claims arising where companies do not do so lawfully, whether in breach of data protection legislation or in a discriminatory way. And biometric data claims – which might derive from the use of medical data, e.g. in the Healthcare sector, or from the use of facial recognition technology as many companies seek to create touch-free interfaces post COVID-19, are likely to be fruitful, as are child privacy issues. Recently, the English court allowed the service of a claim against the US, Chinese and Cayman Island entities within the TikTok group alleging the unlawful collection of children's information, again in the form of an opt-out representative action.

How are damages assessed?

Unlike shareholder claims, loss of control of data claims are not yet at a stage where there are judicially endorsed methodologies for assessing damages. "This will become a key battleground and defendants will need to draw on methodologies in other areas, such as competition and IP claims," Scott says.

The measure of damage will depend on the type of claim (contract, tort, etc.). But where data has been monetised, is the award fair compensation for what the data subject has lost? Or the value of the confidential information? And that leads us to the question of what is data worth? Is it the market value? Should it reflect any gain that the defendant has made in respect of the use of the data? What is already clear, is that data claimants are entitled to compensation for material or non- material damage suffered. So, we have seen awards that encompass not only damages for distress, but for reputational damage too.

Clifford Chance surveyed the position across Europe and has seen a variety of awards. "We have seen some really counter-intuitive judgments, claims involving medical data for several hundred euros and claims involving much less sensitive data with awards in the several thousands," she says.

"When looked at in a class action context, where you may have thousands to millions of claimants, this emerging jurisprudence will have a huge impact on the scale of claims. And with that prize in sight, I don't think that we will see funders losing interest in data claims any time soon," she adds.

The US has seen a number of high-profile cases, including a USD 650 million class settlement against Facebook for improper use of facial recognition technology, which was distributed amongst 1.5 million Facebook users; and a USD 92 million class settlement against TikTok for improper use of biometric data for ad targeting, which was distributed amongst 89 million TikTok users. "While the US is an obvious hotspot where data claims have led to class action awards in the hundreds of millions of dollars, all across the EU we are seeing an uptick in claims," says Ian Moulding.

The Netherlands has become Europe's leading jurisdiction for class actions on data, anti-competitive behaviour and environmental issues following a fundamental overhaul of the system in 2020. "The old system had no mechanism to deal with parallel or overlapping class actions, nor was there a preliminary or certification phase in which issues of admissibility and viability of the action could be dealt with. Now the system allows relief in the form of monetary damages, but at the same time provides better safeguards against unmeritorious and overlapping actions. It also contains judicial scrutiny of the funding mechanisms and the level of influence a funder is allowed to have," explains Daan Lunsingh Scheurleer, a Clifford Chance litigation Partner based in Amsterdam.

He adds: "This new system has attracted quite a lot of attention, which has led to the influx of claimant firms into the jurisdiction. Quite a few actions have been filed, but because the judicial wheels turn slowly, not that many outcomes have become apparent yet. It

would seem that the courts are taking a more stringent stance to the collective action mechanism than before the law was changed."

Environmental claims

Amongst recent cases in the Netherlands is the landmark judgment by the District Court of The Hague which ordered Royal Dutch Shell (RDS) to reduce its CO2 emissions by 45% by 2030, as compared with 2019 levels. The ruling sets a precedent for other companies that could face similar lawsuits. The case was brought by the Dutch branch of Friends of the Earth (Milieudefensie), a number of other NGOs, and over 17,000 individual claimants.

"Class actions can be used as a vehicle for various types of actions against various types of defendants, so you have claims by NGOs and individuals against governments seeking an order to implement legislation and policies that, for instance, should lead to reduction of greenhouse gas emissions," says Lunsingh Scheurleer. "There are many ongoing matters relating to climate change or climate risk in many jurisdictions worldwide. It's a very dynamic area of the law."

These include:

- Claims by NGOs and individuals against governments seeking an order to implement legislation and policies that will lead to a reduction of GHG emissions.
- Claims by NGOs and individuals against companies seeking an injunction to reduce GHG emissions or to define reduction targets.
- Claims by investors against companies and their boards arguing that the company should adopt reduction targets or increase their targets and come up with revised business plans dealing with the challenges of climate change and energy transition.
- Claims by investors against companies and their boards alleging that the company did not in fact fulfil its promises around ESG and climate themes or that its disclosures about how the company is dealing with climate risk were insufficient and that they have incurred losses as a result.

"In terms of actions against companies, there seem to be some fundamental issues emerging, one of them being whether this is a matter for the courts or not. In New Zealand, a court ruled that a climate change case was a matter for the legislator, not for the courts, because the courts are not equipped to deal with the wide-ranging and multifaceted considerations that need to be taken," says Scheurleer.

Dealing with litigation risks outside the US – some tips

Outside the US, there is far less group litigation. However, the risk is growing. "Claimant law firms are better organised, better funded and more proactive than they were a decade ago. The sums of money at stake in these claims are significant, these claims are complex, high value and expensive to defend, and the risk is real," says Kelwin Nicholls. A few practical tips for reducing litigation risk include:

- Companies need to be careful about generic statements. They can be misunderstood and misused against you. They can be applied malleably to specific issues you have not thought about. "I would think carefully about what they add to the company's investor relations strategy. And I would think about the legal risk they present. If you want to portray your company as a good corporate citizen, you are probably better off doing that in specific, measurable, auditable terms," he says.
- There is a tendency for people to over-correct when the company or individual feels it is being unfairly attacked, by special interest groups, parts of the media, short sellers, activist shareholders or other vocal critics. "It is natural to stand up to criticism, and sometimes to get your message across you can be tempted to overreach so that the gap between your critics' misleading picture and your version of reality really stands out. But that is risky. Because if you go too far, you risk misleading investors, and the fact that you were just trying to correct

someone else's misleading impression in the other direction won't get you very far as a defence."

- Many shareholder claims grow out of settlements of regulatory or government investigations. "You obviously need to take a view on litigation risk when settling these cases. That's a well-known issue. Settling regulatory and government investigations is generally a good idea for companies – very few companies litigate against regulators and government authorities. As follow-on litigation risk grows, over time, one day we may reach a point where follow-on litigation risk means that it is a good idea to litigate regulatory and government investigations."
- And finally, take advice. The provisions for issuer liability in FSMA have a defence for companies that can prove they reasonably believed their statements were true – acting on advice from specialists can help to set up that defence. Claims based on negligence come down to whether the company acted reasonably – acting on advice will help protect against liability in tort. In the *Sharp v Blank* claim against the directors of Lloyds, the Court recognised that directors aren't required to be experts in everything, they can legitimately rely on advice from specialists and experts. Advice is there to protect you, so make sure you get good advice," Nicholls says.

CONTACTS

Ian Moulding
Partner
London
T: +44 207006 8625
E: ian.moulding@
cliffordchance.com

Kelwin Nicholls
Partner
London
T: +44 207006 4879
E: kelwin.nicholls@
cliffordchance.com

Kate Scott
Partner
London
T: +44 207006 4442
E: kate.scott@
cliffordchance.com

Daan Lunsingh Scheurleer
Partner
Amsterdam
T: +31 20 711 9047
E: daan.lunsinghscheurleer@
cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

2204-000778