
# International D&O Update

## Recent global developments and their impact on D&Os and insurers

December 2018

*With contributions from our Legalign Global partner firms*

wotton kearney

# Contents

# Introduction

There have been some interesting international developments that are changing the landscape for D&O insurers. In this first edition of our international D&O newsletter, we bring together new cases and regulatory developments that will impact insurers both here in Australia and across the globe with contributions from our Legalign Global alliance partners.

The cyber insurance industry is growing rapidly in response to the increasingly digital global business landscape. In the US, Europe and Canada, precedents are being set through new cases and regulations with the effect that directors and officers are increasingly being held responsible for managing and protecting the data their companies acquire. Our Legalign Global colleagues at Wilson Elser in the US describe these new developments and explain how this impacts D&O insurers.

The MasterCard intercharge fees class action is likely to be the largest class action in UK history – if it is allowed to proceed, that is. The English Court of Appeal will soon decide whether the case, involving approximately 42.6 million class members seeking damages estimated at £14 billion, is suitable for collective proceedings under the *UK Consumer Rights Act 2015* "opt-out" collective redress scheme. Given the UK's traditionally stringent approach to collective proceedings, the impact of the Court of Appeal's decision could be the trigger for a change to the current class action and D&O insurance landscape. Our colleagues at DAC Beachcroft in the UK highlight some of the issues for us.

With the increasing number of law firms and litigation funders competing with each other in open class representative proceedings, the recent decision of the Full Federal Court of Australia in *GetSwift* has provided some welcome clarity about the principles the Court should consider when deciding how to address overlapping class actions.

As Yen Seah and I from Wotton + Kearney's Financial Lines practice point out, the Full Federal Court's comments will be put to immediate use when the Supreme Court determines what to do with the five separate securities class actions commenced on an open basis against AMP Limited this year.

In the US, there is some good news for D&O insurers with a new case affirming that US Security and Exchange Commission settlements are "penalties" as opposed to "loss" under an insurance policy. As Jonathan Meer from Wilson Elser in the US describes in his article, this will be welcome news for insurers but the saga is far from over.

Turning to Europe, the "Cum-Ex" trading scandal has implicated European, Canadian and Australian banks in share trading controversies involving illegal tax refunds that may have cost Germany and other countries up to €55 billion. Investigations into more than 100 banks will likely result in many D&O prosecutions. Our Legalign Global colleagues at BLD Bach Langheid Dallmayr in Germany describe the scandal and outline the implications for insurers.

We hope that you find the articles in this newsletter interesting and helpful. Please let us know if you have any questions or if you need any clarification about these issues.

**Cain Jackson**
Partner & Financial Lines Practice Leader

**T:** +61 3 9604 7901
**E:** cain.jackson@wottonkearney.com.au

AUSTRALIA

# Positive class action developments for D&O insurers

Full Federal Court gives guidance on what should happen when there are competing open class actions against one respondent.

***Perera v GetSwift Limited* [2018] FCAFC 202**

### AT A GLANCE

- D&O insurers in Australia have welcomed the recent Full Federal Court decision in the GetSwift case[1]. The decision is helpful for D&O insurers because it provides some clarity on how the Court should exercise its power to permanently stay competing open class actions and allow only one open class action to proceed against a respondent.
- The Court decided that there was no "one-size fits all" principle to assess which open class action should proceed and which should be stayed.
- The Court expressed a clear preference for a selection process that maximises the likelihood of the best outcome for the applicant and group members, rather than simply the lowest cost, while also maintaining a healthy level of competition amongst funders and lawyers.

## The issue

### What happens where there are competing open class actions against one respondent?

The increasing prevalence of multiple, open securities class actions in Australia has been an issue for some time. However, 2018 has seen the issue assume greater significance with many instances of competing securities class actions being commenced this year on an open class basis. This creates an overlap of group membership across each of the competing class actions and presents significant case management challenges for the Court and parties. The high water-mark, and a clear sign that the issue needed addressing, was the commencement of five separate securities class actions on an open basis this year against Australian financial giant AMP Limited regarding the same issues and substantially the same time period. The collective view of stakeholders is that a solution, or at least some firm direction from the courts or legislature, is desperately needed. That direction has now arrived in the form of the *GetSwift* decision.

## The case

### Seeking a permanent stay of two of three open class actions

The *GetSwift* decision involved three competing open securities class actions, with essentially the same facts and allegations, against logistics technology company GetSwift Limited. GetSwift sought a permanent stay of two of the three actions on the basis that they were an abuse of process because:

- GetSwift should not be forced to defend multiple proceedings regarding the same issues, and
- multiple proceedings are not in the interests of group members when one open class action was capable of vindicating all of their rights and interests.

[1] *Perera v GetSwift Limited* [2018] FCAFC 202

In the past, competing class actions have been resolved either by agreement between applicant groups (and, specifically, their respective lawyers and funders) allowing the consolidation of proceedings into one (for example, *Johnson Tiles Pty Ltd v Esso Australia Ltd*[2]), or by one or more of the competing actions being closed, leaving only one proceeding remaining with an open class of group members (for example, *McKay Super Solutions Pty Ltd (Trustee) v Bellamy's Australia Ltd*[3]).

However, in *GetSwift,* no agreement was reached to consolidate proceedings and no applicant group advanced class closure as a fall-back position. Accordingly, the stay application was run, in essence, on an "all or nothing" basis.

## The decision

### Permanent stay of two of three competing class actions upheld by the Full Federal Court

At first instance, the Federal Court granted permanent stays of two of the three competing open securities class actions. The Full Federal Court upheld this decision (albeit offering differing reasons on some issues) and, in doing so, set out an important set of principles about how stay applications for competing open class actions should be considered and guidance on how a court should assess which of the competing actions remains open and which should be stayed.

The Full Court found that:

- Three class actions brought against the same respondent for substantially the same claims and on behalf of the same group members were likely to involve the increased use of judicial and court resources, move more slowly and less efficiently through the interlocutory stages, and incur increased costs for both the applicants and respondent
- The Federal Court has power to permanently stay competing class actions, and
- The judge, at first instance, appropriately exercised his powers to stay two of the three competing class actions by considering all of the circumstances of the case, including:
  - the position of each of the three open class actions (noting none advocated for a closed class as a fall-back position)
  - the relevant interests of justice
  - the interests of the respondent in having to deal with multiple class actions regarding the same matter (involving increased legal costs and exposure to adverse costs orders)
  - the interests of the applicants and group members
  - the broader interests of ensuring that class actions are run expeditiously and cost-efficiently, and
  - the available alternative remedies available, which include declassing and class closure.

Just as importantly, the Full Court went on to consider the first instance judge's decision to choose one action over the other two. The first instance judge found in favour of one action because that action was "very likely, in most scenarios at all stages of the proceeding, to produce a better return for group members".

The Full Court did not disturb the first instance judge's decision in respect of the "winning" open class action, but it did make some very important observations about the process that should be adopted by suggesting that the first instance judge's approach, while open, should not be slavishly followed or adopted as the "right" way.

### No "one size fits all" solution, but guidance on the selection process

The Full Court acknowledged that "there is no one right answer to case management questions that arise when dealing with competing class actions. There cannot be a 'one size fits all' and different judges will take a different view of some of the incommensurable and conflicting considerations that may arise. It should be kept in mind that there is no 'silver bullet' solution to case management problems of competing class actions and each of the 'solutions' can be said to have some or other problem."

---

[2] (1999) ATPR 41-679
[3] [2017] FCA 947

Having made that general observation, and having identified some of the problems with each of the case management methods available to manage competing class actions, the Full Court highlighted the following considerations which ought to be taken into account in the selection process:

- The Court should not give undue focus to lower costs and funding charges as doing so is likely to promote a "rush to the bottom" by funders and solicitors keen to win the tender. Specifically, the Court should "focus less on achieving the lowest possible costs and funding charges in any selection process, and more on selecting the proceeding with a funding and costs model likely to best motivate the applicant's solicitor and funder to work assiduously to achieve the best outcome for the applicant and group members and to take responsible risks in that regard."
- The Court should be astute to select the proceeding with the legal team that is "most likely to achieve the largest settlement or judgment, i.e. the most experienced and capable."
- The Court must strongly discourage a rush to court in large and complex proceedings by dispelling any perceived "first mover advantage."
- As the selection process is conducted in full view of the respondent, it is likely that the respondent "will obtain a reasonable understanding of the approximate size of the 'war chest' available for the case against it", with the risk the respondent's solicitors can use this information to their strategic advantage. The Full Court emphasised that the Court should be careful to avoid the interests of the applicant and group members being damaged in this way (although precisely how is unclear).
- The costs associated with stay applications and consequences for unsuccessful lawyers and funders are undesirable and may lessen competition, which has been "the single most important matter giving rise to reduced costs".

> The Full Court acknowledged that "there is no one right answer to case management questions that arise when dealing with competing class actions."

## Implications for class action respondents and their D&O insurers

For five key reasons, the *GetSwift* decision is significant for class action respondents and their D&O insurers.

1. **It provides much needed guidance on the relevant principles, procedures and probable outcomes where a respondent is met with competing open class actions.**

   The recent commencement of five separate open class actions against AMP Limited highlights the need for the guidance provided by the *GetSwift* decision. Importantly, AMP's application for a stay of the multiple open class actions against it (essentially, the same application sought in *GetSwift*) will be heard by the Supreme Court of New South Wales on 6 and 7 December 2018 and will provide a working example of case management principles for competing open class actions post-*GetSwift*.

2. **The GetSwift decision highlights the Federal Court's concern about case management principles being compatible with sustainable funding models and balancing the interests of both group members and respondents.**

   The Full Court was at pains to emphasise the importance of avoiding (or at least discouraging) a "race to the bottom" in both speed of commencement of proceedings and offering the cheapest funding model. The Full Court flagged the obvious problems with the Court favouring the quickest and cheapest class action vehicle in its selection process. The Full Court expressed a clear preference for a selection process, which maximises the likelihood of the best outcome for the applicant and group members rather than simply the lowest cost, while also maintaining a healthy level of competition amongst funders and lawyers.

3. **The decision places the onus on class action lawyers and funders to address the case management issues created by competing open class actions and find a solution or risk having their action stayed.**

   While the manner in which interested parties will respond remains to be seen, the decision still represents a significant shift that considerably simplifies matters for respondents.

4. **It highlights the significance and acceptance of common fund orders as the preferred method for open class actions.**

   Common fund orders are relatively new to the Australian landscape and permit a litigation funder to recover a contribution towards its commission and fees from all group members, irrespective of whether a group member has entered into a funding agreement. The Full Court emphasised the benefits and compatibility of a common fund order with a singular (as opposed to competing) open class action.

5. **Finally, the decision demonstrates why class action litigation in Australia remains a challenge for D&O insurers and their advisers.**

   While the *GetSwift* decision is obviously a positive one, it highlights the uncertainty confronted by all class action participants as jurisprudence develops and solutions are found by the courts through their case management powers.

## Contacts

For more information please contact:

**Cain Jackson**
Partner, Wotton + Kearney (Melbourne)
**E:** cain.jackson@wottonkearney.com.au

*Cain is the Head of Financial Lines for Wotton + Kearney in Australia and New Zealand and is a D&O and class action specialist. He is currently acting for a number of global primary D&O insurers in several of Australia's biggest securities class actions.*

**Yen Seah**
Senior Associate, Wotton + Kearney (Melbourne)
**E:** yen.seah@wottonkearney.com.au

*Yen is a key member of Wotton + Kearney's Financial Lines team and has experience with large-scale litigation, including class actions and other proceedings arising from major corporate collapses. She has been involved in a number of high-profile Australian securities class actions.*

UNITED STATES

# SEC settlement is a "penalty" not a "loss"

***J.P. Morgan Sec., Inc. v Vigilant Ins. Co.*, 2018 N.Y. App. Div. LEXIS 6130**

**AT A GLANCE**

- The Vigilant case in the US has held that an SEC settlement is "penalty" rather than a "loss" under an insurance policy.
- The case clarifies contrary opinions on whether a SEC settlement is excluded under a policy because it is a "fine or penalty" or is "uninsurable at law".
- This is an important clarification for D&O and financial institution insurers as it will minimise their exposure under policies.

In the United States, few claims are more chilling to a D&O and financial institutions insurer than an investigation and enforcement action against its insured by the US Securities and Exchange Commission (SEC). SEC enforcement actions, and the potential for the SEC to extract a significant civil settlement, can take down an entire tower of insurance – even if that tower is eight or even nine figures high. For example, in July 2010, Goldman Sachs agreed to pay US$550 million to settle allegations brought by the SEC that it had misled investors into purchasing a subprime mortgage product as the housing market bubble in the US began to burst. At the time, the SEC settlement was the largest in its 76-year history.[4] Enforcement actions in the US by the SEC continue unabated and the recent settlements have increased significantly, as evidenced by the Goldman settlement and a number of others.[5]

## Insurers' arguments against policy coverage for SEC settlements

Unless there are facts that trigger one of the policy's exclusions, or policy application issues, insurers generally use three primary arguments against coverage for SEC settlements.

The first two arguments are based on the policy's typical definition of "loss," which includes judgments and settlements, but generally expressly excludes "fines and penalties" or "matters which are uninsurable under the law". Unless some portion of the settlement is expressly defined as a "penalty" the provision rarely applies to the entire SEC settlement. As to the uninsurable nature of these settlements, insurers typical argue that, because the SEC is empowered to recover "disgorgement" from alleged securities violators, any judgment or settlement of that judgment is not insurable. Disgorgement is the repayment of ill-gotten gains ordered by a court.

The third argument is based on the policy's "conduct" exclusions (i.e., the personal profit and fraud exclusions). However, under today's policy language, these exclusions typically require a final adjudication and have no application to settlements. Accordingly, for any portion of a governmental settlement that is not specifically labelled as a "penalty," often the insurer's sole defence is that they were uninsurable.

## The no "loss", therefore "uninsurable at law" argument

In the early 2000s, coverage decisions favouring the insurers on the no "loss" argument, like *Level 3* and *Conseco* (involving civil securities cases), were helpful to US insurers in class action situations and in dealing with governmental settlements by finding that these settlements were uninsurable as a matter of law.[6]

---

[4] See, https://www.sec.gov/news/press/2010/2010-123.htm.

[5] For example in 2016, Merrill Lynch paid an SEC settlement of US$415 million (https://www.sec.gov/news/pressrelease/2016-128.html). In 2018, Transamerica paid US$97 million (https://www.sec.gov/news/press-release/2018-167), and Deutsche Bank paid US$75 million (https://www.sec.gov/news/press-release/2018-138). Most recently, Yahoo! and Tesla paid US$35 million and US$20 million, respectively.

[6] See, *Millennium Partners, L.P. v. Select Ins. Co.*, 68 A.D.3d 420, 889 N.Y.S.2d 575 (1st Dept. 2009), appeal dismissed, 14 N.Y.3d 856, 927 N.E.2d 558 (2010); *Reliance Group Holdings v.*

For example, in *J.P. Morgan Sec., Inc. v. Vigilant Ins. Co.*, the SEC commenced an investigation in 2003 to examine whether Bear Stearns had violated the securities laws between 1999 and 2003 for allegedly knowingly facilitating "late trading" and deceptive "market timing" for certain hedge fund customers. Ultimately, in 2006, Bears Sterns agreed to pay a SEC settlement "disgorgement" of US$140 million[7] (without admitting or denying the findings), plus another US$90 million in a civil money penalty.[8] Obviously, the US$90 million portion of the settlement was not covered as a "penalty".

For the US$140 million portion of the settlement, the insurance tower refused to indemnify Bear Stearns, arguing the settlement represented "disgorgement" of monies improperly obtained by Bear Stearns and not "loss" (therefore "uninsurable as a matter of law") under the policy. At the first appeal hearing in 2011, the New York appellate court held that the monies were not insurable under New York Law.[9]

However, in 2013, on the second appeal to New York's highest court, the New York Court of Appeals reversed this judgment, finding the insurer's failed to meet the burden of proof that the US$160 million settlement was uninsurable as a matter of law. The case was then sent back to the trial level court for reconsideration.

In 2017, the trial court found that the US$140 million disgorgement settlement was insurable loss under the policy. The insurers appealed this decision yet again. However, while this appeal was pending, in *Kokesh v. Securities Exchange Commission*,[10] the US Supreme Court conclusively defined the nature of the SEC disgorgement remedy as a "penalty" because it:

1. is imposed for a wrong committed to the public, rather than one against any particular individual,
2. is meant to punish and deter other possible offenders, and
3. does not compensate the victims, but is paid out at the Court's discretion.

When the insurer's appeal was before the first level New York appellate court, the *Kokesh* decision was available to it. On 20 September 2018, the *Vigilant* Court held that, because the insurer's policies exempted "penalties" from the definition of "loss" (as opposed to "matters which are uninsurable under the law"), and because the *Kokesh* decision held "disgorgement" is a "penalty," the US$140 million settlement was not covered under the insurer's policies. It states:

> *"The United States Supreme Court has thereby made clear that SEC disgorgement is a penalty because it punishes a public wrong, and its purpose is deterrence, whether you are remitting your own ill-gotten gains or those you generated for your customers through violations of the securities law, even if you did not directly share in those profits."*

## Implications for insurers

The *Vigilant* decision is particularly important because, in recent years, courts have undercut insurers' arguments that disgorgement is "uninsurable".

First, certain US courts have held that under the relevant state law, disgorgement is insurable – and insurers could have expressly included language that excluded disgorgement from being covered under the policy.[11]

Second, other US courts have rejected the disgorgement/"no loss" argument because the policy contains a "personal profit" exclusion and the disgorgement argument has been deemed to be an "end-run" around the exclusion's final adjudication requirement.[12]

*National Union Fire Ins. Co*., 188 A.D.2d 47, 55, 594 N.Y.S.2d 20 (1993); *Vigilant Ins. Co. v. Credit Suisse First Boston*, 6 Misc.3d 1020, aff'd in part, modified in part, 10 A.D.3d 528, 782 N.Y.S.2d 19 (2004).

[7] The disgorgement order was actually for US$160 million but Bear Stearns did not seek coverage for US$20 million of that settlement, which represented its own "ill-gotten gains".

[8] In any proceeding, the SEC is empowered to seek injunctive relief (such as bar orders and suspensions), monetary civil penalties (pursuant to 15 U.S.C. §77t(d)), and to order disgorgement as an exercise of their "inherent equity power to grant relief ancillary to an injunction". *Kokesh, infra,* 137 S.Ct. at 1640. See also, "Remedies and Relief in SEC Enforcement Actions" (October 3, 2018): https://www.sec.gov/news/speech/speech-peikin-100318.

[9] N.Y. law. 91 A.D.3d 226.

[10] 137 S.Ct. 1635 (2017).

[11] See for example *Cohen v. Lovitt & Touche, Inc*., 233 Ariz. 45 (Ariz. App. 2013); *U.S. Bank,* 2014 U.S. Dist. LEXIS 91335, in which the Court found no Delaware cases holding *that* disgorgement *is* uninsurable as a matter of law *and Burks v. XL Specialty Ins. Co***.**, 534 S.W.3d 458 (Tex. Ct. App. 2015), where the Court noted "the lack of any Texas authority holding that insuring against disgorgement is against public policy".

[12] Insureds have successfully argued that the policy does directly address the issue of "disgorgement" through the Personal Profit Exclusion, which expressly requires a "final adjudication" in the underlying case – or it doesn't apply.Several courts have adopted this policyholder argument: *U.S. Bank v. Indian Harbor Ins. Co*., 2014 U.S. Dist. LEXIS 91335 (D. Minn. July 3, 2014); and *Gallup, Inc. v. Greenwich Ins. Co*., 2015 Del. Super. LEXIS 129 (Del. Super. Feb. 25, 2015).

The *Vigilant* decision emphatically holds that if the SEC is seeking disgorgement as a remedy, it is a "penalty." Accordingly, the only monetary relief that the SEC can pursue is either for a civil penalty[13] or for disgorgement. Because both of these monetary remedies are "penalties," the typical D&O policy's definition of "loss" would exclude coverage. After *Vigilant*, for any SEC monetary settlement, the insurer's main argument moves from disgorgement being "uninsurable" to the settlement simply being a "penalty" and not "loss" under the policy.

It must be noted that Bear Stearns has filed a Motion for Reconsideration of the Court's decision in *Vigilant* or, in the alternative, an appeal to New York's highest court, so this saga is far from over. We will keep our readers updated on any future decision by these New York courts.

## Contact

For more information please contact:

**Jonathan Meer**
Partner, Wilson Elser (New York)
**E:** jonathan.meer@wilsonelser.com

*Jonathan represents the interests of primary and excess insurers based in the United States, China, London and Bermuda in high-exposure claims against directors and officers of public and private companies*

[13] See the cases in footnote 3.

UNITED STATES

# Directors and officers: be wary of growing cyber responsibilities

**AT A GLANCE**

- Actions against directors and officers regarding cyber breaches are on the rise.
- New cyber protection regulations are being introduced around the world.
- Cyber risks for D&Os extend to wearables and products that are connected to the Internet of Things.

Society's increased reliance on doing business online has driven faster communications and efficiencies, as well as increased risks when technology fails or is misused. Directors and officers are often the ones who approve the use of technology, and there is a growing trend to hold them personally liable when things go wrong.

Cyber exposure for businesses has increased in the past couple of years and the laws and regulations are starting to catch up. This exposure has been in the form of data breaches and the subsequent data restoration and notification costs, as well as in lawsuits and government regulations. Recent lawsuits targeting D&Os for their alleged failure to address cyber risk provide examples of potential liability as more regulations are passed in the United States and around the world. D&Os should be aware of the informal and formal standards that are being set regarding appropriate company cyber risk management.

## Lawsuits against D&Os in the US related to cyber risk

Private actions aimed to hold D&Os accountable for cyber risk in the United States is nothing new. Securities class action lawsuits, such as those against Wyndham, Heartland Payment and Target, were brought alleging breach of fiduciary duty when handling a cyber breach.[14]

Specifically, the allegations in these actions against the D&Os were for failing to:

1. implement and enforce effective internal controls over data security
2. disclose the effectiveness of a company's data security policies
3. disclose the scope of the data breach, and
4. exercise oversight duties on how a security breach could adversely affect the company's business.

These claims often focus on alleged breach of duty when there is a failure to adequately implement cyber security defence in the first place, or involve failing to respond to, and otherwise monitor, cyber security plans after a breach has occurred. What these referenced cases have in common is that they were all defended and dismissed without any liability to the D&Os.

The success of the D&Os' defences in these matters has not stopped more lawsuits from being filed or stopped D&Os from settling cases alleging breach of fiduciary duty regarding cyber risk. The D&Os of Home Depot were successful in defending such a claim, but chose to settle the matter when the dismissal was appealed.[15] The D&Os of Wendy's, while their motion to dismiss was pending, also chose to settle.[16] It remains to be seen how the D&Os of Yahoo, Equifax, and Google will respond to the pending claims against them for alleged cyber security failures.[17]

[14] *Wyndham - Dennis Palkon, et al. v. Stephen P. Holmes, et al.* 14-cv-01234, (U.S. District Court for the District of New Jersey); *In re Heartland Payment Systems, Inc*., 09-CV-01043 (U.S. District Court for the District of New Jersey); Target - *Mary Davis et al. v. Gregg W. Steinhafel et al.*, 14-cv-00203, (U.S. District Court for the District of Minnesota).

[15] *In Re The Home Depot, Inc. Shareholder Derivative Litigation*, 15-CV-2999 (U.S. District Court for the Northern District of Georgia).

[16] *Graham, et al. v. Nelson Peltz, et al.*, 16-cv-1153, (U.S. District Court for the Southern District of Ohio).

[17] *Madrack v. Yahoo! Inc., Marissa Mayer, et al.*, 17-cv-0037 (U.S. District Court for the Northern District of California); *Kuhns v.*

## Regulations impacting corporate cyber risk

Coupled with these recent cases are new government regulations to which D&Os must respond regarding corporate responsibility and disclosure on cyber risk. While the European Union's General Data Protection Regulation (GDPR) has received most of the headlines, there have been other regulations in the United States and Canada that are impacting D&Os.

### The EU General Data Protection Regulation

The GDPR, effective May 2018, has been a big topic of discussion because it addresses, amongst other things, information collected and data breach responsibilities. A recent 2018 Advisen survey, reported that nearly 40% of large companies, defined as over US$1 billion in revenue, have made changes to how they deal with cyber issues as a result of the GDPR.[18]

As the GDPR focuses on the control, processing, and use of the data and information of European Union citizens, D&Os are the ones responsible for implementing the corporate governance framework. Article 5(2) of the GDPR says that the "controller shall be responsible for, and be able to demonstrate compliance with, [the other data protection principles]".

> Cyber risks are growing by the day and, with them, potential liability for D&Os.

Article 24 describes in greater detail the responsibility of the controller, which includes implementing "appropriate technical and organisational measures to ensure and to be able to demonstrate the processing is performed in accordance with this regulation".

Article 37 of the regulation requires that certain businesses designate a data protection officer who must report to the highest level of management, operate independently, and have adequate resources to carry out their tasks. Since the GDPR has been in effect only for a couple of months, it remains to be seen how it will be enforced.

### The New York State regulation

Another recent cyber regulation is from the New York State Department of Financial Services (NYSDFS) for companies in its jurisdiction. Under 23 NYCRR Part 500, effective in March 2017, New York provided clear notice that it intends to hold directors and officers more responsible for ensuring that their companies are undertaking more active assessment of their own security policies and procedures.

These include the enactment of a comprehensive cybersecurity policy, a written incident response plan that reports breaches within 72 hours to the NYSDFS, and security policies for third-party service providers who access non-public information. The new rules also put more responsibilities on directors and officers, requiring not only the designation of a chief information security officer but also board certification to the NYSDFS of compliance with the regulations. As of 3 September 2018, regulated entities are required to:

1. maintain financial and cyber audit trails
2. maintain written procedures for evaluating, assessing, or testing cybersecurity
3. maintain policies and procedures on secure disposal on a periodic basis of non-public information no longer necessary for business operations
4. have a training program to monitor activity of authorised users, and
5. have encryption controls to protect non-public information held.

By 1 March 2019, the transition period under the NYSDFS regulation will be over and compliance with the full cyber regulation will be required.

### Californian regulation

Another impending regulation in the United States is the *California Consumer Privacy Act* (CaCPA), which was passed on 28 June 2018, and will be effective 1 January 2020, with enforcement by 1 July 2020.

Businesses that collect from or sell personal information about California consumers must comply with the CaCPA. The regulated businesses subject to the CaCPA also must:

1. have annual gross revenue of $25 million
2. collect personal information from at least 50,000 consumers, households, or devises, or
3. obtain at least 50 percent of annual revenue from selling consumers' personal information.

---

*Equifax, Inc., et al.*, 17-cv-3463, (U.S. District Court for the Northern District of Georgia); *Mawardy v. Alphabet, Inc.*, et al. 18-cv-5704 (U.S. District Court for the Eastern District of New York).

[18] 2018 Advisen *Information Security and Cyber Risk Management* survey available at https://www.zurichna.com/en/knowledge/articles/2018/10/eighth-annual-advisen-information-security-and-cyber-risk-management-survey

Similar to the GDPR, the CaCPA was designed to give Californian residents control over the use, including the sale, of their personal information. One key aspect of the CaCPA is that a business cannot provide a different level or quality of services based on a consumer objecting to their sale of the data, except where it is "reasonably related to the value provided to the consumer by the consumer's data". Since the CaCPA will not be in effect until 2020, there are likely be further clarifications to its regulations.

### Canadian regulation

The most recent cyber protection law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), effective 1 November 2018, is a Canadian law that applies to the collection, use and disclosure of personal information in the course of commercial activities in all of Canada. Foreign and domestic organisations subject to PIPEDA will be required to:

1. notify individuals about privacy breaches when there is "a real risk of significant harm to an individual"
2. keep records of such breaches, and
3. report cyber breaches to the Canadian Government.

Failure to comply can lead to fines up to CAD$100,000. While this potential fine is far less than that levied by the GDPR, the regulation still has some teeth. The regulations in the EU, Canada, New York, and, soon California, stress to D&Os the importance that governments are putting on cyber security.

## Why this matters to D&Os and insurers

While the advantages of the internet usually outweigh the potential liabilities, D&Os need to be aware of the risks posed by cyber exposure. It is important to implement written policies and procedures, and training, to provide guidance to officers and employees on applicable threats. They should also address measures to prevent, detect, and respond to such threats, and to monitor compliance with cybersecurity policies and procedures.

The risks are not limited to a company's computers. They also exist in the company's use of wearables and products that are connected to the Internet of Things. Exposure to cyber security threats exists everywhere, so what is disclosed to shareholders and the public by D&Os about these risks takes on heightened importance.

Cyber risks are growing by the day and, with them, potential liability for D&Os. Being aware of the changing standards of care and rules and regulations around the world is an essential first step for D&Os in serving the best interests of their companies.

## Contact

For more information please contact:

**Jim Thurston**
Partner, Wilson Elser (Chicago)
**E:** *james.thurston@wilsonelser.com*

*Jim Thurston is a coverage lawyer who focuses his practice on insurance and bad faith litigation in the professional liability field.*

WILSON ELSER

wotton kearney

UNITED KINGDOM

# Class actions in the English Courts

## An update on how the Courts are viewing collective proceedings

***Case Lloyd v. Google* [2018] EWHC 2599**

**AT A GLANCE**

- The UK may see the largest class action in its history if the Court of Appeal agrees that the MasterCard intercharge class action is "suitable" for collective proceedings under the "opt-out" collective redress scheme.
- However, while MasterCard reflects the Court's understanding of the "difficulty of bringing individual claims in consumer cases generally", the decision in the Google privacy workaround case made it clear that if some of the claimants suffer no damage, they could not be considered to have the "same interest" as the rest of the class members.
- These are important cases for D&O insurers because of their scale under the opt-out scheme.
- The MasterCard and Google decisions cast an interesting light on the English judiciary's approach to collective redress.

## The "opt-out" collective redress scheme for competition claims is about to be tested

### The MasterCard interchange fees case may be the largest class action in UK history

Following the EU Commission decision in July 2015[19] that interchange fees charged by MasterCard on the use of its debit and credit cards were anti-competitive and in breach of EU legislation, consumers are seeking to bring a class action against MasterCard. There are approximately 46.2m class members seeking damages estimated at £14bn.

The UK's *Consumer Rights Act 2015* introduced an opt-out collective redress regime for competition claims. This allows a claimant representative to bring an action on behalf of a group of individuals where it follows an "infringement decision" or "an alleged infringement" of anti-competitive behaviour prohibited by the *Competition Act 1998* or EU law.

The opt-out nature means that claimants are included in the group unless they expressly opt-out. However, claims can only proceed if they are certified as being suitable by the Competition Appeal Tribunal (CAT). This requires a formal hearing before the CAT to determine:

- whether the claims raise the same, similar or related issues of fact or law, and
- it is "just and reasonable" that the person representing the class is a suitable representative.

If the stringent eligibility criteria is met, a collective proceedings order is issued and the class action may continue.

Since the legislation was introduced, no case has been certified as "suitable", but this may be about to change. Last month in a landmark judgment, the English Court of Appeal ruled that it will hear an appeal challenging the CAT's refusal to grant a collective proceedings order in the MasterCard battle.

If the appeal is successful, the largest class action ever brought in the UK will be allowed to continue.

[19] The EU Commission Press Release Antitrust: "Commission sends Statement of Objections to MasterCard on cross-border rules and inter-regional interchange fees" available at: http://europa.eu/rapid/press-release_IP-15-5323_en.htm.

### How the case came about

Representative, Walter Merricks, applied for a collective proceedings order allowing him to bring an "opt-out" class action on behalf of all UK consumers who purchased goods and services sold by businesses accepting MasterCard between 1992 and 2008.

In July 2017, the CAT rejected the application due to the scale and size of the class. It held that it would be unworkable to calculate an individual's actual purchases and the different levels of pass through of the interchange fee for the various retailers in the UK over the 16-year period. Accordingly, there was no way of calculating the losses suffered by the claimants on an aggregate or individual basis. The CAT also held that there was no right to appeal its decision.

Mr Merricks sought the permission of the Court of Appeal to hear an appeal on grounds the CAT's decision was wrong in law. Last month, the Court unanimously ruled that it has jurisdiction to hear appeals from CAT decisions under the collective regime and granted permission. The appeal is set for the first week in February 2019.

## Google and the Safari workaround to bypass security settings

### A breach without damage is insufficient to invoke representative actions

It is alleged that in 2011/2012, Google obtained information about an individual's internet usage through cookies without their knowledge or consent, bypassing Safari's privacy settings. Litigation was commenced earlier this year against Google in the English Courts seeking to establish a class action for affected users with damages alleged of up to £3bn. The case, *Lloyd v. Google*[20], went before the High Court in England in October. The Court decided that the requirements for a collective action were not met and the action could not proceed on that basis.

The representative claimant sought damages from the alleged breaches of data protection principles set down in the *Data Protection Act 1986*. Section 13 of the Act provides data subjects with a means to obtain compensation where they have suffered damage as a result of breaches.

Although the case did not determine the merits of the alleged claim, the judge did accept that a claim might succeed. However, in this case, the claimant had not sought to allege what harm had occurred. Instead, it was alleged that commission of the breach was sufficient to obtain damages. This was rejected.

### Not "the same interest"

The way in which the claim was pleaded may have been driven by an attempt to persuade the Court that the claim should be permitted to continue as a representative action. To proceed, a representative claimant must have "the same interest" in the claim as those in the class to be represented. The Court held that this was not met in this case. Many claimants would have suffered no damage at all, and those who had suffered damage would not have suffered the same damage, given that each person's position is inherently fact-specific. Had the Court been persuaded that damages could be claimed simply by reference to the breach, then the issues relevant to the representative action application would have been different – all claimants would have suffered from the same breach.

In its judgment the Court expressed the following view about the attempt to bring a claim on an opt-in representative class basis in this case.

> *"It would not be unfair to describe this as officious litigation, embarked upon on behalf of individuals who have not authorised it, and have shown no interest in seeking any remedy for, or even complaining about, the alleged breaches…. the Representative Claimant should not be permitted to consume substantial resources in the pursuit of litigation on behalf of others who have little to gain from it, and have not authorised the pursuit of the claim, nor indicated any concern about the matters to be litigated."*

## What does this mean for D&O insurers?

In the MasterCard litigation, the claimants will still need to persuade the Court that the eligibility criteria have been met for a collective proceedings order and the CAT's refusal was wrong in law.

There are some indications in the judgment that the Court may be more sympathetic than the CAT when applying the criteria. It appreciates that aggregate damages is a new remedy that is a critical component of the new regime for competition claims, and it is fully alive to the "difficulties inherent in the bringing of individual claims" in consumer cases generally. However, in the Safari Workaround litigation, there is a clear indication of the English Court's approach more generally to actions that seek collective redress on an opt-out basis.

[20] [2018] EWHC 2599

## Contacts

For more information please contact us.

**Graham Ludlam**
Partner, DAC Beachcroft (London)
**E:** gludlam@dacbeachcroft.com

*Graham Ludlam is a partner in DAC Beachcroft's Global Insurance Group and Co-Head of the D&O / Financial Institutions Service Line.*

**Francesca Muscutt**
Professional Support Lawyer, DAC Beachcroft
**E:** fmuscutt@dacbeachcroft.com

*Francesca Muscutt is a professional support lawyer for the D&O / Financial Institutions Service Line.*

GERMANY

# Trading scandal in Germany and Europe engulfs more than 100 banks

**AT A GLANCE**

- The Cum-Ex trading scandal in Germany and Europe is becoming an international sensation – and a huge challenge for financial institutions and the insurance industry.
- Investigations into more than 100 banks are likely to have significant financial impact.
- There have already been a number of claims against banking directors and officers in Germany, and it seems inevitable that there will be many more.

After recent news reports in Europe, international impact of the German "Cum-Ex" trading scandal has reached a large audience. Not only Germany was harmed by this international tax fraud. Many other countries were victims as well. And it seems the nightmare for banks, brokers and wealthy clients continues. There are even allegations by tax authorities and prosecutors that Australia's Macquarie Bank participated. The German subsidiary of Macquarie Bank in Munich, offices of the law firm Freshfields, and offices of a number of other banks were recently searched by public prosecutors.

Following the financial crisis, scandals involving banks and financial institutions have almost become common place in Germany. But the so-called "Cum-Ex" deals are overshadowing all previous controversies because of the sums involved and the number of banks implicated. It is reported that up to 100 banks are under investigation by the German and other European tax authorities regarding "Cum-Ex" deals. These deals involve illicit tax refunds that may have cost Germany and other countries up to €55 billion.

## Background to the scandal

German authorities are investigating allegedly tax-driven share transactions, executed by banks between 2001 and 2012, trading on their own account or on behalf of third parties, around the time of the dividend record date of German stock-listed companies.

"Cum-Ex" trades involved the acquisition of shares with (cum) dividends due on or just before the dividend record date and delivery of these shares after the dividend record date without (ex) dividends.

This made it possible to obtain multiple returns of capital gains tax that had been paid to the German tax authorities only once.

The authorities are also investigating "Cum-Cum" deals, which involved the short-term transfer / loan of shares owned by a foreign company or investor to a domestic German bank that subsequently applied for a tax refund on the dividend, which would not have been available to the foreign company / investor.

> It is reported that up to 100 banks are under investigation.

Both models were carried out by German banks with counterparts primarily in the London market and by US pension funds. The authorities are also examining the roles of various accountancy firms and law firms (especially Freshfields) who were involved in the development of the tax models that were used. New information shows the systematic approach of some key individuals involved – including "test runs" in various countries, expert opinions confirming the legality of such deals, the foundation of subsidiaries, and even the creation of bogus pension funds.

"Cum-Ex" trading was formally prohibited in Germany in 2012 but continued in other European countries because Germany apparently did not fully share its knowledge. Even now, news reports suggest that the barriers set up by the German legislator still appear to be insufficient. Only a few days ago the German press revealed a new "Cum-Ex" model that the German Treasury Secretary only recently stopped.

## Investigations continue

The investigation in Germany is politically charged, given the number of state-owned banks involved and the fiscal scandals involving many other banks, internationally, over the last decade.

A German parliamentary enquiry committee has been established to investigate the scandal. The committee has interviewed a number of bank CEOs and politicians about their roles in the scandal. In addition, public prosecution departments in Germany acquired data storage devices containing transaction data of a number of German banks and international banks acting in Germany. This has given fresh impetus to the "Cum-Ex" investigations and authorities have commenced many new preliminary investigations. Pressure on some key individuals led to the first confessions, which seem to have helped authorities understand the complex transaction structures.

Approximately 100 banks (both German and international) have been the subject of the investigations. Institutions that are in the public focus are private banks Sarasin and Warburg, the North Channel bank, international banks UniCredit/HypoVereinsbank and Société Générale, state-owned banks WestLB and HSH-Nordbank, as well as the European branch of Canada's Maple-Bank and Australia's Macquarie Bank.

The scandal is likely to have a significant financial impact. Maple Bank has already filed for bankruptcy as a result. On the basis that the authorities are treating the "Cum-Ex" trades as tax evasion, they can potentially go back 10 years and seek financial recourse regarding profits previously deemed secure and closed. "Cum-Cum" deals were carried out for much longer.

## The issue for D&O insurers

For D&O insurers, this topic highlights the issues of risk-control at financial institutions. Some banks have initiated internal investigations and repaid tax refunds – which has already led to several claims against directors and officers in Germany. For example, UniCredit/HypoVereinsbank brought claims for damages amounting to €180 million against three former board members for their role in shaping the bank's policy on "Cum-Ex" trading.

It seems inevitable that similar claims by other banks and institutions might follow as the investigations and scandal unfolds further, particularly given the media attention and the ongoing investigations by German authorities.

BLD's Financial Lines team has been dealing with Cum-Ex related matters for several years.

## Contacts

For more information please contact us.

**Bastian Finkel**
Partner, BLD Bach Langheid Dallmayr
**E:** bastian.finkel@bld.de

*Bastian Finkel is a partner and co-head of BLD Bach Langheid Dallmayr's Financial Lines team in Cologne, Germany. He deals with all matters of D&O-insurance, liability and risk management for international D&O-insurers.*

**Franz König**
Senior Associate, BLD Bach Langheid Dallmayr
**E:** franz.koenig@bld.de

*Franz König is a senior associate of BLD Bach Langheid Dallmayr's Financial Lines team in Cologne, Germany and is mainly involved in cases of financial institutions and cyber.*


Shaping the future of insurance law

## Australian Offices

**Sydney**
Level 26, 85 Castlereagh Street
Sydney NSW 2000
T: + 61 2 8273 9900

**Melbourne**
Level 15, 600 Bourke Street
Melbourne VIC 3000
T: +61 3 9604 7900

**Brisbane**
Level 23, 111 Eagle Street
Brisbane QLD 4000
T: +61 7 3236 8700

**Perth**
L1/Suite 1, Brookfield Place Tower 2
123 St Georges Tce Perth WA 6000
T: +61 8 9222 6900

## New Zealand Offices

**Auckland**
Level 18, Crombie Lockwood Tower
191 Queen Street, Auckland 1010
T: +64 9 377 1854

**Wellington**
Level 13, Harbour Tower
2 Hunter Street, Wellington 6011
T: +64 4 499 5589

**www.wottonkearney.com**

wotton kearney

A founding member of LEGALIGN GLOBAL