Feature

KEY POINTS

- It is easiest to establish jurisdiction when the financial institution is domiciled within England and Wales (hereafter, for brevity only "England") or there is a jurisdiction agreement in favour of England (which is common).
- In the event that the litigant is based outside England but in the EU, jurisdiction is governed by the Brussels 1 Regulation (Recast).
- In the event that the litigant is based outside England and outside the EU, jurisdiction is governed by the Civil Procedure Rules Pt 6.
- Applicable law is governed by the Rome I Regulation, for contractual disputes, and the Rome II Regulation, for non-contractual disputes; in most cases, the parties will have chosen the applicable law.
- One of the key advantages of Group Litigation Orders under CPR Pt 19 is that the costs of common issues can be shared between all of the parties to the order; however, this is a developing area of English law such that one cannot predict with certainty how, in practice, such a claim will proceed.

Authors Sir Richard Aikens and Andrew Dinsmore

Cybersecurity litigation: jurisdiction, applicable law and class actions

This article considers the establishment of English jurisdiction, the rules on the applicable law to a cybersecurity action and the procedures for a Group Litigation Order.

INTRODUCTION

There have been a number of high profile cyber-security breaches recently, for example the Cambridge-Analytica breach in the US which has led to a Class Action for approximately US$71bn. This article is further to 'The legal implications of cybersecurity breaches for financial institutions' [2017] 11 JIBFL 676 in which we considered the four potential legal bases under which a financial institution may be liable for a cybersecurity breach in England and Wales where they have failed to maintain adequate security software: contract, tort, breach of statutory duty and actionable rights under EU law.

This article seeks to address three practical questions that a litigant may have:

- can I establish jurisdiction in England if I wish to do so;
- what is the applicable law; and
- would it be possible to bring the action by way of a Group Litigation Order (in much the same way as the Class Action in the Cambridge-Analytica case).

JURISDICTION

The question of whether a court in England and Wales has jurisdiction to hear a dispute over cybersecurity breaches will be governed by the Brussels 1 Regulation (Recast) (BIR)[1] and the Civil Procedure Rules, Pt 6. There are three scenarios:

- where the financial institution is domiciled within England;
- where the financial institution is domiciled outside England but within the EU; and
- where the financial institution is domiciled outside England and outside the EU.

Domicile is governed by Art 62 of the BIR, for natural persons, and Art 63 of the BIR, for legal persons. As most financial institutions are legal persons, it is important to consider Art 63 of the BIR which makes clear that legal persons are domiciled where they have their:

- statutory seat;
- central administration; or
- principal place of business.

In the event that the legal person is domiciled in England, the English courts will have jurisdiction under Art 4 of the BIR and the legal person can be served as of right.

In the event that the financial institution is domiciled outside England but within the EU, the BIR applies to determine which court has jurisdiction. If the parties have a contract with a jurisdiction agreement in it which is in favour of England (as is often the case), the English courts will have jurisdiction under Art 25 of the BIR; in this regard, the English High Court has recently confirmed that asymmetrical jurisdiction clauses[2] fall within Art 25.[3]

In the more unusual event that there is no jurisdiction agreement between contracting parties, it is important to note the following provisions:

- If the cause of action is contractual, the courts of the place of performance of the obligation in question will have jurisdiction (Art 7(1)(a) of the BIR). In a services contract this will be the member state where, under the contract, the services were provided or should have been provided (Art 7(1)((b) of the BIR).
- If the cause of action is tort, delict, or quasi-delict, the courts having jurisdiction will be in the member state where the harmful event occurred or may occur (Art 7(2)).[4]
- If the dispute arises out of the operations of a branch, agency or other establishment, jurisdiction will lie with the courts of the member state where the branch, agency or other establishment is situated (Art 7(5)).

It is often the case that several member states have jurisdiction and should a litigant delay in bringing their action, there is a risk that they will be second seized and thus, if the causes of action are identical, the court will have to stay proceedings until the court first seized concludes on whether it has jurisdiction.[5] If the causes of action are related, the court second seized has a discretion to stay such proceedings.[6]

Feature

Biog box
Sir Richard Aikens, based at Brick Court Chambers, is a former Lord Justice of Appeal who now works as an arbitrator in international commercial disputes. He is also a Visiting Professor at King's College London and Queen Mary University of London and one of the editors of Dicey, *Morris & Collins Conflict of Laws*. Email: richard.aikens@brickcourt.co.uk

In the event that the financial institution is domiciled outside England and also outside the EU, the litigant will have to obtain the permission of the court to serve out of the jurisdiction[7] through establishing that a jurisdictional gateway is fulfilled[8] and establishing that England is clearly the more appropriate forum.[9]

GOVERNING LAW

The rules for determining the applicable law are found in the Rome I Regulation (Rome I), for contractual causes of action, and the Rome II Regulation (Rome II), for non-contractual causes of action.

In relation to contractual causes of action, parties to the vast majority of financial contracts expressly choose the applicable law, which will be applied in accordance with Art 3(1). In the absence of an express choice the applicable governing law will be determined as follows:

- For a service contract, it will be the law of the country where the service provider has its habitual residence: Art 4(b) of Rome I.
- For a contract concluded within a multilateral system which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments, as defined by Art 4(1), point (17) of Directive 2004/39/EC, in accordance with non-discretionary rules and governed by a single law, the contractual obligations shall be governed by that law: Art 4(h) of Rome I.
- If a contract does not fall into either of these categories, it will be governed by the law of the country where the party required to effect the characteristic performance of the contract has its habitual residence: Art 4(2) of Rome I.
- However, if it is clear from all the circumstances of the case that the contract is manifestly more closely connected with a country other than that indicated in under Art 4(1) and 4(2), the law of that other country shall apply: Art 4(3) of Rome I.
- Finally, where the law applicable cannot be determined pursuant to paras 1 or 2 of Art 4, the contract shall be governed by the law of the country with which it is most closely connected: Art 4(4) of Rome I.

As to non-contractual causes of action:[10]

- The law applicable to a non-contractual obligation arising out of a tort/delict shall be the law of the country in which the damage occurs, irrespective of the country in which the event giving rise to the damage occurred and irrespective of the country or countries in which the indirect consequences of that event occur: Art 4(1) of Rome II.
- However, where the person claimed to be liable and the person sustaining damage both have their habitual residence in the same country at the time when the damage occurs, the law of that country shall apply: Art 4(2) of Rome II.
- Finally, where it is clear from all the circumstances of the case that the tort/delict is manifestly more closely connected with a country other than that indicated in Art 4(1) or Art 4(2), the law of that other country shall apply. A manifestly closer connection with another country might be based in particular on a pre-existing relationship between the parties, such as a contract, that is closely connected with the tort/delict in question: Art 4(3) of Rome II.

GROUP LITIGATION ORDERS

Once a litigant has established that the English court has jurisdiction, they will have to consider the most appropriate means of bringing the action. In the context of cybersecurity breaches, there are three options:

- they could bring the action on their own;
- they could bring an action along with other claimants on a single claim form under CPR r 19.1 where such claims "can be conveniently disposed of in the same proceedings"; or
- they could apply for a Group Litigation Order under CPR r 19.10-r 19.15 and Practice Direction 19B.

The advantage of bringing an individual action is that one retains complete control over the manner in which the litigation progresses but the main disadvantage is that the individual will be liable for the entirety of the costs should the litigation be unsuccessful, which may be of particular importance where the loss suffered by an individual is relatively low, as may be the case in a cybersecurity breach.[11]

As a result, our view is that the more attractive option is that litigants will seek to bring an action by way of a single claim form or by way of a Group Litigation Order (GLO), which is the English equivalent to the US Class Action. The key difference between commencing by way of a single claim form and obtaining a GLO is that in the case of the single claim form the legal representatives must obtain authority from all potential claimants before commencing proceedings, which may be very difficult or, in some cases, impossible; further, the process for adding further claimants at a later stage is more complex and costly because court permission is required for every addition.[12]

Thus, it is likely that a GLO will be more appropriate and the test for this procedure is whether "common or related issues" of fact or law exist between the claims (CPR r 19.10 and r 19.11). In a cybersecurity breach, it may be that common legal issues are best dealt with by way of a GLO with the specific factual issues to be determined by further, individual actions.[13]

An application for a GLO should be made by way of an application notice (CPR PD19B, §3.1). CPR PD19B, §3.2 provides that the following should be included in the application notice or in the written evidence in support:

- the nature of the litigation in summary;
- the number and nature of the claims already issued;
- the number of parties likely to be involved;
- the common issues of fact or law; and
- whether there are any matters that distinguish a smaller group of claims within the wider group.

When a GLO is ordered by the court, CPR r 19.11(2) provides that the order should contain directions about the establishment of a register on which the GLO claims will be managed, specify the GLO issues and specify the court that will manage the claims. The GLO may then also give directions for publication under CPR r 19.11(3)(c)[14] so that further claimants can apply to join the register of claimants.[15]

As to statements of case, PD19B, §14.1 makes clear that the management court may direct that there be a "Group Particulars of Claim" which contains: (i) the general allegations relating to all claims, and (ii) a schedule containing entries relating to each individual claim specifying

Biog box

Andrew Dinsmore, based at 20 Essex Street, is a barrister practising in International Commercial Litigation and Arbitration. He regularly acts in banking and financial matters; his recent work includes a number of urgent freezing injunctions and Norwich Pharmacal Orders in the context of cyber-fraud. Email: adinsmore@20essexst.com

which of the general allegations are relied on and any specific facts relevant to the claimant. These directions should include directions as to whether such a "Group Particulars of Claim" is to be verified by a statement of truth and, if so, by whom.[16]

CPR r 19.13 provides for wide-ranging case management powers, including the power to appoint a lead solicitor under CPR r 19.13(c) which the CPR notes is "invariably necessary" (CPR, §19.13.2)[17] and the power to include a "cut off" date, at r 19.13(e), by which all claimants should be added;[18] although it may not be fatal if that date is missed[19] and the court may give permission for the "cut off" date to be extended.[20]

Any judgment entered under a GLO is binding on all those claimants that are then on the register (CPR r 19.12(1)(a)) and the court may direct the extent to which judgments are binding on future parties that enter on the GLO register (CPR r 19.12(1)(b)). Any party that is adversely affected by the judgment or order which is binding on him may seek permission to appeal the order under CPR r 19.12(2).

As to the costs in a GLO, there will be individual and common costs. An example of the latter is the costs of the lead solicitor (CPR r 46.16 and PD 19B.16), which should render the litigation much less financially burdensome for an individual litigant than being exposed to liability for the full costs. In the event that the GLO is unsuccessful, the claimants are likely to pay a share of the defendants' costs severally and equally.

CONCLUSION

Upon establishing jurisdiction and determining the applicable law, litigants to a cybersecurity action should consider applying for a GLO. Given that GLOs are much less common than US Class Actions, it is difficult to say with certainty precisely how such a case might progress. Nevertheless, in our view, a cybersecurity breach following inadequate software security is a paradigm case where such an order should be considered by future litigants given the potential costs savings for individuals. ■

1 The jurisdictional rules about bringing proceedings against defendants who are domiciled in an EU state may, of course, change following Brexit because the UK will no longer be a member state of the EU and thus such regulations will no longer apply to it: see Aikens and Dinsmore, 'Jurisdiction, Enforcement and the Conflict of Laws in Cross-Border Commercial Disputes: What are the Legal Consequences of Brexit?' (2016) 27 (7) EBLR 903.

2 An asymmetrical jurisdiction clause will normally require that the borrower bring its action against the financial institution in a specific jurisdiction but allows the financial institution to bring an action against the borrower in any competent jurisdiction.

3 See *Commerzbank Aktiengesellschaft v Liquimar Tankers Management Inc and another* [2017] EWHC 161 (Comm); it is unclear whether the CJEU would take the same view given different approaches in other member states, eg in France in *Mme X v Société Banque Privé Edmond de Rothschild 13, First Civil Chamber*, 26 September 2012, Case No. 11-26022.

4 It is interesting to note that the test of the applicable law is the place where the damage occurs whereas the test for the establishment of jurisdiction is the place where the harmful event occurred; thus, one may have different outcomes depending on whether the issue is applicable law or establishing jurisdiction.

5 See Art 29 of the BIR.

6 See Art 30 of the BIR.

7 One exception to this is where jurisdiction is established under a jurisdiction agreement that complies with Art 25 of the BIR; the key point to note is that Art 25 applies where the parties have selected a member state, eg England, "regardless of their domicile" and thus can apply where neither party is domiciled in a member state. In such circumstances, jurisdiction is established under the BIR and there is no need for permission to serve out of the jurisdiction: CPR r 6.33(2)(b)(v).

8 See CPR, Practice Direction 6B, para 3.1.

9 See *The Spiliada* [1987] A.C. 460.

10 Parties can expressly choose the law applicable to torts under Art 14 of Rome II but this is rare in practice.

11 In the *Cambridge Analytica* case, for example each individual claimant is seeking US$1,000 as permitted by statute, although it is the fact that there are 71 million litigants which means the total damages are in the billions.

12 The process to add claimants to a claim form is found at CPR r 19.4.

13 For a recent example of such an approach in the context of financial mis-selling see *Arif v Berkeley Burke Sipp Administration Ltd* [2017] EWHC 3108 (Comm), §34-35; PD19B, §15.2 states that the common issues and test claim will normally be tried in the management court with individual issues tried at other courts whose locality is convenient for the parties.

14 For example on claimants' solicitors websites, in the Law Society Gazette and in the media.

15 A list of GLOs can be found here: https://www.gov.uk/guidance/group-litigation-orders#list-of-all-group-litigation-orders

16 PD19B, §14.2.

17 Cf *Hutson and others v Tata Steel UK Ltd and others* [2017] EWHC 2647 (QB) where Turner J refused an application by a firm to be added as further lead solicitors because allowing another lead solicitor would increase costs, increase the risk of delays, misunderstandings and disagreement relating to the management of claims (§12). Further, an increase in the number of lead solicitors would be likely to increase the demands of the court's resources (§23).

18 In *Holloway and others v Transform Medical Group (CS) Ltd and others* [2014] EWHC 1641 (QB), §§22-24, 30 the court refused to add further claimants and emphasised that the purpose of the "cut off" date is to promote good management of the claims and that the appropriate test was that contained within relief from sanctions under CPR r 3.9. See also the approach taken in *Kimathi and others v Foreign and Commonwealth Office* [2017] EWHC 939 (QB). See further PD19B, §§13-14.

19 See *Taylor v Nugent Care Society* [2004] EWCA Civ 51.

20 See *Pearce v Secretary of State for Energy and Climate Change* [2015] EWHC 3775 (QB).

Further Reading:

- The legal implications of cybersecurity breaches for financial institutions (2017) 11 JIBFL 676.
- The strengthening of jurisdiction agreements following Brussels Reg (Recast) and the impact of Brexit (2017) 8 JIBFL 476.
- LexisPSL: Financial Services: Information and cyber security for financial services firms – overview.