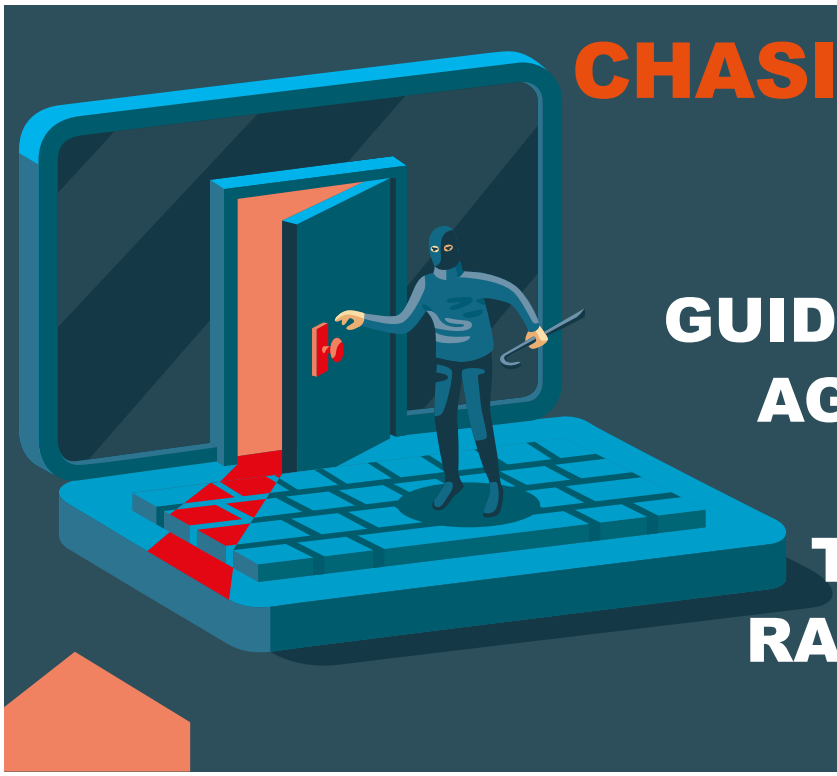


CHASING SHADOWS

A WHISTLESTOP GUIDE TO LITIGATING AGAINST PERSONS UNKNOWN IN THE CONTEXT OF RANSOMWARE AND CYBER FRAUD

Authored by: Maria Kennedy (Barrister) - Twenty Essex

Introduction

This is a whistlestop guide to the various stages of seeking relief against persons unknown in the context of ransomware and cyber fraud. It is intended to give the reader a flavour of the relevant considerations at each step in light of recent legal developments and set out some predictions for the future.

Key takeaways for claimants

- Provide a clear definition of "persons unknown" which is sufficient to identify those who are included and those who are not.
- In addition to relief against the persons unknown, consider what information about the persons unknown and the whereabouts of any stolen property can be sourced from third parties (e.g. banks and cryptocurrency exchanges).
- Consider what other measures are necessary, e.g. a private hearing, protection of court papers and permission to serve out of the jurisdiction and by alternative method. Bear in mind the new gateway at CPR PD 6B, paragraph 3.1(25) which has made serving Norwich Pharmacal and Bankers Trust relief out of the jurisdiction easier.
- Predictions for the future – broadening in scope of parties against whom claimants will typically seek third party disclosure orders and more resistance from e.g. cryptocurrency exchanges who are increasingly becoming respondents to such orders.

Defining 'persons unknown'

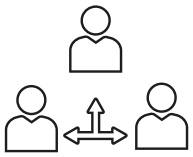
The procedure for commencing a claim against "persons unknown" is the same as against a named defendant, save that the first step will be to define the defendant. In this regard, "the description used must be sufficiently certain as to identify both those who are included and those who are not" (Bloomsbury Publishing Group Limited and JK Rowling v News Group Newspapers Ltd [2003] 1 WLR 1633 at [21]). For a recent example of the jurisdiction being deployed in the context of ransomware, see Ince Group Plc v Person(s) Unknown [2022] EWHC 808 (QB).

Relief against persons unknown

The nature of the relief will typically flow from the type of attack perpetrated. For example:

1. **Ransomware cases:** The claimant will typically seek a prohibitory injunction preventing the publication of data, and a mandatory injunction requiring the defendant to deliver up and/or delete the data and serve evidence detailing their compliance; see e.g. Ward Hadaway v Persons Unknown (Unreported, 11 July 2022). Where a non-publication injunction is sought, the claimant will need to bring the Court's attention to Article 10 of the European Convention on Human Rights (freedom of expression). If this right "might" be affected, the Court will consider whether the test at section 12 of the Human Rights Act 1998 has been satisfied. In practice, this is unlikely to be engaged in ransomware cases; see Ince Group at [8]-[9].

2. **Where property has been stolen:** The claimant's priority will typically be to recover its property (through a proprietary injunction), prevent dissipation (through a worldwide freezing injunction ("WWFO")) and seek ancillary disclosure. When applying for a WWFO, claimants should note that it is "a typical feature of a persons unknown case" that there is unlikely to be much evidence of the defendant's assets, although this should not bar the grant of a WWFO; see Ion Science v Persons Unknown (Unreported, 21 December 2020) at [18].



Relief against third parties

Claimants seeking more information to recover property stolen by persons unknown will typically use the same application to apply for a Norwich Pharmacal order (seeking information about the identity of the defendant) and/or a Bankers Trust order (seeking information about the stolen property) from third parties, e.g. the fraudster's bank or cryptocurrency exchange, who will appear as defendants on the Claim Form.

Practical considerations

1. **Proceeding without notice:** Although the issue is always fact-sensitive, in urgent injunction applications it is generally appropriate to proceed, in the first instance, without notifying the defendant (Ince Group, [4]). In seeking this measure, applicants will need to bring the Court's attention to: (a) the urgency of the application; and (b) the full and frank disclosure (defined at 1356-1357 of Brink's Mat Ltd. v Elcombe [1988] 1 WLR 1350).

2. **Private hearing:** To ensure that the application does not prompt persons unknown to take steps to undermine any relief granted, claimants will typically ask for a private hearing pursuant to the Court's discretion under CPR 39.2; see e.g. Ince Group at [3] and AA v Persons Unknown [2020] 4 WLR 35 at [24].

3. **Treatment of confidential evidence:** CPR PD 25A, paragraph 5.1(2) lists the documents which must be served on the respondent where the injunction has been made without notice. However, where these documents contain confidential information which the defendants are liable to misuse or which highlights the claimant's vulnerabilities, the Court will typically order that it be withheld or served in a redacted form; see e.g. Ward Hadaway at [9] and Ince Group at [14]. In certain cases, the Court will also order that the names of the claimant's solicitors and counsel be redacted; see e.g. 4 New Square v Persons Unknown (Unreported, 28 June 2021) at [8].

4. **Access to the court file by third parties:** As a further precaution, typically in ransomware cases, the court has held it is "strictly necessary" that no copies of the documents on the court file will be provided to any non-parties without further order and that any non-party seeking access to such documents must make an application; see e.g. Ward Hadaway at [8], 4 New Square at [3] and Ince Group at [15].

5. **Anonymity:** Where there is something particular about e.g. the claimant's work which might prompt third parties with malign intent to contact the persons unknown and seek to exploit the claimant's situation, the claimant may also seek an order under CPR 39.2(4) anonymising their identity; see XXX v Persons Unknown [2022] EWHC 1578 (QB). However, the mere fact that a business may suffer negative commercial and reputational consequences if the ransomware attack/cyber fraud becomes public is not automatically a sufficient reason to make an anonymity order (XXX at [25]).

6. **Service:** As the claimant will typically be unable to pinpoint the location of the persons unknown, they should apply for permission to serve out of the jurisdiction and by alternative means. Although previously there was some uncertainty as to when Norwich Pharmacal and Bankers Trust orders could be served on defendants out of the jurisdiction, claimants have recently welcomed the introduction of the new gateway at CPR PD 6B, paragraph 3.1(25), which is specifically directed at service of such orders out of the jurisdiction; see the application of the gateway in LMN v Bitflyer Holdings Inc [2022] EWHC 2954 (Comm).

Long-term considerations

Once the initial relief has been obtained and continued at a return date, the Court will typically question how the claimant plans to 'close out' the proceedings, given that persons unknown are very unlikely ever to participate. In such circumstances, the claimant will need to apply either for default judgment or summary judgment. The decision will depend on the claimant's priorities, with default judgment often being the cheaper option and summary judgment being the option selected by claimants who prioritise enforcement out of the jurisdiction.

Direction of travel

With the increasing provenance of cyber fraud and ransomware attacks, courts are evidently keen to help claimants and deter fraudsters. In this context, we are likely to see an increase in the provenance of third party disclosure orders (e.g. against email providers and social media platforms) and further resistance from cryptocurrency exchanges, who (with the advent of the new gateway) are now more exposed to third party disclosure applications.