haynesboone

November 28, 2018

# Why English Courts are Prepared to Assist Cyber Victims

By: Fiona Cain

Cybercrime is a growing problem for individuals and companies, and law firms are no exception. The Solicitors Regulation Authority, in its risk outlook report[1] in July, considered cybersecurity to be a significant increasing concern for the legal profession so much so that it identified cybersecurity as a separate risk for the first time. This is not surprising when in 2017 £10.7 million of client money was reported as lost to cybercrime. The PwC Law Firms' Survey 2018,[2] which was published last month, highlights that cyberattacks are a major threat for law firms because "firms hold significant client funds and information that is attractive to fraudsters and other criminals."

The risk outlook report advises that the most common type of cybercrime encountered by law firms is where criminals intercept and falsify emails between a client and the firm, or even within the firm, which results in money being transferred to the criminals. Law firms need to be vigilant and try to prevent cyberattacks and ensure that everyone in the firm knows how to recognize the signs of email modification fraud and common phishing scams. The SRA risk outlook report and the PwC Law Firms' Survey recommend that law firms prepare to respond to a cyberattack and deal with it in their business disaster recovery and business continuity plan.

In the unfortunate event that a law firm becomes a victim of cybercrime, in addition to reporting it to the relevant authorities,[3] and informing the SRA and the clients affected by the cybercrime, the firm should also consider whether it is appropriate to take steps in the courts to limit the consequences of the cybercrime.

The English courts can issue a freezing order to prevent any stolen money from being disposed of or a prohibitory injunction to restrain the cybercriminal from publishing the information obtained on social media or elsewhere on the internet. However, as these interim measures and the court rules that must be satisfied in order to obtain such orders from the court existed long before cybercrime, this may not at first appear to be straightforward. A number of cases before the English courts over the past year in particular illustrate how some of the hurdles that previously existed for victims of cybercrime have been dealt with by the courts and have made it easier to obtain a freezing order or injunction in these circumstances.

**Identity of the Defendant**

The biggest difficulty with cybercrime and pursuing an interim remedy in the court is identifying the cybercriminal. It is important to remember that it is not a requirement of the Civil Procedure Rules for the defendant to be named.[4] Nevertheless, a description of the defendant that is as clear as possible is required and while a defendant may be referred to as a "person or persons unknown," it is essential that further information is provided in order to identify them, for example those "responsible for demanding money from the Claimant on 27 February 2018"[5] or "who has or have appropriated, obtained and/or may publish information unlawfully obtained from the Claimant's IT systems."[6]

**Identity of the Claimant**

The victim of cybercrime may wish to ask the court to anonymize the firm's identity, sit in private and/or restrict access to the court file. This may be important so as not to give notice to the hackers[7] of the steps that the claimant is taking or to cause reputational damage to the victim.

**Alternative Service**

In order to pursue court proceedings, the applicant is obliged to bring the court documents to the attention of the defendant. With cybercriminals, normal methods of service are generally ineffective because the identity of the cybercriminal and therefore his “usual or last known residence” is unknown. The English courts have been willing over the past 10 years to move with the times and have permitted alternative service by Twitter,[8] Facebook,[9] text message,[10] email,[11] and most recently via Facebook Messenger, WhatsApp and through access to a virtual data room.[12] This has meant that in cases where the cybercriminal has issued a ransom or sent messages which have led to monies being diverted, the court is likely to assist the applicant by allowing alternative service by this method.

**Failure of the Defendant to Engage — Meeting the Required Standard**

It is not surprising that in cases of this nature that the defendants do not engage with the court proceedings. This is not fatal to a claim but the court must be satisfied that on the balance of probabilities the claim has been made out. It should be remembered that in cases of fraud “cogent evidence is typically required in order to satisfy that burden of proof”[13]. As fraud cases typically depend on the drawing of inferences, it is important that the court is presented with sufficient evidence to enable it to draw reasonable inferences.

**Failure of the Defendant to Engage — No Cutting Corners**

Where the defendant fails to engage with any proceedings, there is a temptation to cut corners, however, it is important that the claimant ensures that the case is still fairly presented. This requires the claimant to draw to the attention of the court “points, factual or legal, that might be to the benefit of” the defendant.[14] In the case of CMOC Sales & Marketing LTD and Persons Unknown and 30 others, where the claimant succeeded in obtaining a worldwide freezing order in respect of monies that had been stolen by cybercriminals, the court commented that in that case there was “(a) scrupulous attention to detail and to the requirements of the very many applicable procedural rules, and (b) rigorous observance of the obligations of material disclosure on the many without notice applications on the part of solicitors and counsel involved for the claimant, and the obligations of fair presentation otherwise. There have been no short cuts taken and no glossing over of any problematic points.”

**Failure of the Defendant to Engage — Derogating from the Principle of Open Justice**

The courts may, particularly when there is a series of applications in relation to the same data breaches and the defendant chooses not to engage, decide that it does not require further hearings but can deal with the matter "on the papers." This was what happened in Clarksons,[15] when the court granted an injunction to protect the claimant from the hackers’ blackmail demands, following the theft of significant confidential data. The court, after careful consideration, derogated from the "open justice" principle in order for the case to be dealt with "on the papers" and without a public hearing. While recognizing that open justice is a fundamental principle, the judge set out guidance for these types of cases, explaining that the court was content to hear the case "on the papers" because: (a) a hearing would have added to the expense of the claim, without serving any useful purpose; (b) the hacker did not engage in the proceedings, and so did not oppose the application; and (c) there had been two earlier public hearings, and the judgment would be published online.

**Be Prepared for the Defendants' Next Move**

Where information is stolen and a ransom issued, the defendant may go on to carry out its threat, for example by posting the stolen information on the internet. This is what happened in the case of *PML v. Person(s)*

*Unknown*, where in response to being served with an English court injunction for nondisclosure (at the same email address from which the blackmail demands were made) and a similar order being obtained abroad where the website host was based to require the hacker's website to be blocked, the hacker began posting the stolen information on other websites. When the new website hosts/operators were served with the injunction, the information was quickly taken down. While the injunction did not prevent the perpetrator from posting the stolen information on the internet, it was quickly removed, thereby limiting the harm caused. A similar example was quoted by the SRA in their risk outlook report where sensitive information was stolen from a firm's system following a ransomware attack. The criminals said they would start publishing that information unless they were paid £3 million. As the firm declined to do so, the data was published on Twitter. The firm obtained an injunction from the court to bar anyone from further sharing the information that the hackers had published, as well as successfully securing the removal of information from websites.

It is clear from the above, that the English courts are prepared to assist those that have been the victim of cybercrime in recovering the stolen money and preventing confidential information from being published on social media or elsewhere on the internet. While this is a possible approach once a law firm discovers it has been a victim of cybercrime, law firms, like any individual or company, should take steps to avoid falling victim to cybercrime in the first place.

First published by *Law360* on Nov. 28, 2018.

[1] https://www.sra.org.uk/risk/outlook/risk-outlook-2018-2019.page

[2] https://www.pwc.co.uk/industries/law-firms/pwc-law-firms-survey-report-2018-final.pdf

[3] As to what amounts to a cybercrime, see the CPS' Cybercrime — prosecution guidance: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

[4] *Bloomsbury Publishing Group plc v. News Group Newspapers Ltd* [2003] EWHC 1205 (Ch)

[5*] PML v. Person(s) Unknown* [2018] EWHC 838 (QB)

[6] *Clarksons PLC v. Person or Persons Unknown* [2018] EWHC 417 (QB)

[7] *PML v. Person(s) Unknown* [2018]

[8] *Blaney v. Persons Unknown* (October 2009)

[9] AKO Capital LLP and AKO Master Fund February (2012)

[10] *NPV v. QEL and another* [2018] EWHC 703 (QB)

[11] *PML v. Person(s) Unknown* [2018]

[12] CMOC Sales & Marketing LTD and Persons Unknown and 30 others [2018] EWHC 2230 (Comm)

[13] per HHJ Waksman QC in *CMOC v. Persons Unknown* [2018]

[14] *Braspetro Oil Services v. FPSO Construction Inc* [2007] EWHC 1359 (Comm)

[15] *Clarksons PLC v. Person or Persons Unknown* [2018]