False Evidence: Questioning Document Authenticity in UK Court Proceedings

October 2023

Introduction

"*Disclosure*" is the legal process whereby documents that are relevant to the issues in proceedings are disclosed, or in other words, made available to and exchanged by parties involved in legal proceedings.

Documents must be disclosed if they are relevant to any of the issues in dispute, whether or not those documents adversely affect or support a party's case.

Parties who disclose documents must sign a *Disclosure Certificate*, setting out the party's honest belief in its truth. Any false disclosure statements open parties to contempt of court proceedings where a party makes, or causes to be made, a false disclosure statement, without an honest belief in its truth[1].

Documents may also be disclosed in proceedings where they are mentioned in a statement of case, witness statement or summary, affidavit or expert report[2]. These documents must be verified by a *Statement of Truth* - in the context of litigation, a statement of truth confirms that the facts stated in the document are true, and the party understands that contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by the statement of truth without an honest belief in its truth.

Questioning the Authenticity of a Produced Document – Notice to Prove

A party is *deemed to admit* the authenticity of a disclosed document under Part 31 of the Civil Procedure Rules ("**CPR**") (Disclosure and Inspection of Documents), unless he or she serves a notice seeking to prove the authenticity of that document at trial (*Notice to Prove*).

Under CPR 32.19 (2), a Notice to Prove must be served:

(a) by the latest date for serving witness statements[3]; or

(b) within 7 days of disclosure of the document, whichever is later[4].

The burden of proving the authenticity of disputed documents is on the party who has served the disclosed document(s) and seeks to rely it/them at trial. Parties who query documents that they believe to be falsified are advised to engage the services of a forensic expert.

In *McGann v Bisping* [2017] EWHC 2951 (Comm), the trial judge stressed the importance of ensuring that a Notice to Prove is served within the allowed time-period. Citing *Mumford v HMRC* [2017] UKFTT 19 (TC), the trial judge said, "*Merely putting the other party to poof in a Statement of Case of the authenticity of a document does not satisfy the requirements of this rule* [CPR 32.19]"[5].

The Legal Implications of False Evidence

Where a claimant relies solely on false evidence, the defendant can seek to have the claim struck out (i.e. dismiss a party's case in whole or in part).

As set out above, parties who rely on false evidence, accompanied by a statement of truth, may be in contempt of court (where it is proven beyond reasonable doubt that there has been an attempt to interfere with the course of justice). It is necessary to seek the court's permission to bring contempt of court proceedings.

Anybody found to be in contempt of court, could go to prison for up to 2 years, get a fine, or both.

Knowingly falsifying documents can also amount to a criminal offence in the UK under the Fraud Act 2006. The maximum sentence is 10 years' imprisonment.

[1] CPR 31.23 (1): Proceedings for contempt of court may be brought against a person if he makes, or causes to be made, a false disclosure statement, without an honest belief in its truth; Practice Direction 57AD, paragraph 23: roceedings for contempt of court may be brought against a person who signs, or causes to be signed by another person, a false Disclosure Certificate without an honest belief in its truth.

[2] CPR 31.14: (1) A party may inspect a document mentioned in – (a) a statement of case; (b) a witness statement; (c) a witness summary; or (d) an affidavit(GL); (e) Revoked. (2) Subject to rule 35.10(4), a party may apply for an order for inspection of any document mentioned in an expert's report which has not already been disclosed in the proceedings. (Rule 35.10(4) makes provision in relation to instructions referred to in an expert's report)

[3] CPR 32.19 (2) (a)

[4] CPR 32.19 (2) (b)

[5] It should be noted that in this case, the Notice of Prove was not served in accordance with the requirements of CPR 32.19 (2), but the trial judge used his powers under CPR 3.1(2)(m) and CPR 3.10 to dispense with the service of a notice to prove, and accepted that the authenticity of the documents were being put to the test of authenticity.

Case Law Examples of False Evidence at Trial

Accident Exchange Ltd v Broom & Ors

In *Accident Exchange Ltd v Broom & Ors [2017] EWHC 1096*, forensically-collected evidence from Autofocus Limited ("**AF**") contradicted (and entirely undermined) the defendants' witness evidence.

Accident Exchange ("**AE**") was part of Accident Exchange Group PLC, a specialist car hire and claims management company, whose main business was to hire cars to victims of road traffic accidents. AE operated a fleet of mainstream, specialist and prestige hire vehicles, and provided replacement cars on credit hire terms.

In this particular case, each of the seven defendants were employed as experts at AF. The seven defendants gave expert evidence on behalf of defendant insurers in an effort to reduce insurance claims in County Court litigation.

The evidence provided by AF related to the daily rate of car hire that a car hire company could recover for cars hired on credit hire terms when the driver's own car had been damaged (despite the fact that the driver could have afforded to hire a car on non-credit hire terms). Insurers, who covered the cost of the hire, often challenged the daily rate charge. During the course of the proceedings, it became evident that not only were AF's expert reports inaccurate, but they contained fabricated information.

AF went into liquidation, and the liquidator collected the company's business records, which the court gave the claimants permission to use.

During the course of the claimants' review of AF's documents, it became apparent that AF had verified telephone records for use in various proceedings by signing them with statements of truth when they were false to their knowledge or when they did not believe them to be true. The claimant's review of AF's business records proved that telephone calls never happened on the dates claimed, and where any calls were made, their duration fell below an acceptable threshold for the collection of the evidence on which the defendants sought to rely.

The trial judge concluded that AF was involved in the systematic, endemic fabrication of evidence, in which the Defendants knowingly and actively participated throughout the material time.

Following conclusion of a two-month trial in April 2017, the seven former rates surveyor experts from AF were jailed for between 3 and 14 months. The Defendants were also ordered to pay the claimants' legal costs, which were estimated at £1.5 million.

In similar cases *Archer v Skanska* and *Joyner V Bramley*, which concerned spot hire surveys, the defendants' expert evidence that telephone calls were made on a certain date, was refuted by telephone records and computer records.

44 Wellfit Street Ltd v GMR Services Ltd

44 Wellfit Street Ltd v GMR Services Ltd [2017] EWHC 1841 (Ch) was a matter in which the possession of a commercial property was sought. The defendant claimed that it had a hard-copy version of a lease and an option to purchase the commercial properly in dispute – the claimant argued that the documents upon which the defendant relied were forgeries. The claimant subsequently served a notice to prove. The defendant did not serve its own notice to prove. As there were conflicting versions of several documents, the defendant was deemed to have admitted the authenticity of the claimant's versions.

Several combined factors led the Master of the High Court to opine that the claimant's documents were the authentic versions:

- The defendant did not disclose any original versions of the documents on which it sought to rely;
- The defendant was not able to explain why there were competing versions of emails;
- The defendant disclosed a number of paper copies of emails, letters and the Lease and Option, diary entries;
- The defendant disclosed correspondence between solicitors acting on the sale and purchase of land (but not in connection with the Lease and Option), not having obtained the correspondence it sought to rely upon from the solicitors' file;
- Photographs of screenshots were also disclosed by the defendant, and the phone was said to have been subsequently stolen (the defendant claiming that it had been burgled and that it also had a number of electronic devices and paper documents stolen following a car break-in);
- The defendant's and claimant's versions of documents differed.

The Master of the High Court noted in his judgment that there had been no real effort by the defendant to provide any metadata for the disputed conflicting emails. The claimant, on the other hand, had offered access to the emails in native form so that the metadata could be checked. The Master opined that the defendant's version of emails had been tampered with and that therefore the defendant's documents were false.

Foglia v Family Officer Ltd & Ors

Although not concerning a Notice to Prove, in the theme of false evidence, *Foglia v Family Officer Ltd & Ors [2021] EWHC 650 (Comm)*, a matter in which Fieldfisher represented the claimant, reliance on fraudulent evidence resulted in €15m of the claimant's offshore funds being transferred to the first defendant (a company owned and operated by the fourth defendant). The monies were quickly disseminated between the other defendant companies, who were linked to the fourth defendant. €11.5m was quickly recovered using the Commercial Court's asset tracing and recovery powers, leaving circa €3.5m outstanding. Fieldfisher engaged the services of a forensic expert, having obtained mobile phone location data and emails (which the forensic expert proved to have been spoofed), thus placing the fourth defendant behind the fraud. Relying on the undisputed chronology of false-evidence and links to the fourth defendant, the trial judge granted summary judgment in the sum of €3,543,368 (plus interest), covering the balance of the €15m due to the claimant.

How to spot falsified documents

Incidences of unauthentic documents being produced is becoming increasingly commonplace. From iDiscovery Solutions' and Fieldfisher's perspectives, we have seen opposing parties produce falsified signed contracts, messenger application conversations, as well as emails and other communications between parties.

The fabricated nature of these documents has not been immediately apparent; their appearance and formatting have seemed accurate from an initial glance. More in-depth checks are undertaken when parties to whom these documents were produced have quite rightly reacted with surprise at the appearance of conversations they were never engaged in, and agreements they never signed.

How might the falsified evidence be recognised before trial?

In iDiscovery Solutions' and Fieldfisher's experiences, falsified documents are typically disclosed as a single piece of almost perfect evidence, provided with no native or original version, and when questioned, the suspected document is paired with a complicated backstory.

The following factors should be considered when querying the authenticity of a produced document:

- Where there are no original data sources, i.e. the document is produced as an image or without the original file-type metadata, or where the document is not produced in native form;
- Where the document suggests it should be in the possession of both parties to proceedings, but only the producing party has a copy, i.e. there is only a single source of the produced document;
- Where the context of the alleged falsified data or document is too good to be true insofar as it supports, or even bolsters, the producing party's version of events, or position as to the issues in dispute, yet the receiving party has no knowledge of the document and is met by surprise as to its existence.

What methodologies can be relied upon to dispute the authenticity of a document?

(a) Metadata

Disclosure rules in the Courts of England and Wales require that metadata must be disclosed alongside native documents. Metadata can provide an abundance of information regarding a document's authenticity as long as practitioners know of its existence and how to effectively use it to question the credibility of an opponent's documentary evidence.

Metadata is automatically-created "*data about data*" in hidden from, which provides a document's characteristics and related data such as a document's source, owner, type, date created, date last modified, to list a few examples. Metadata is not limited to documents sourced from computers and can be gleaned from a whole host of media, including but not limited to digital cameras, mobile devices, external drives.

There are two types of metadata: *system metadata* and *application metadata*.

- *System metadata* is rendered from a computer's storage information, which can be relied upon to identify file locations, file names, size and any modifications applied to a document.
- *Application metadata* can be found within a file itself and is most useful in proving the authenticity of a document insofar as it can prove when a file was created, printed, edited and/or accessed. It also displays information relating to document authorship and previous versions of a document. This type of data is embedded within a document and is automatically updated when any changes are applied.

Parties to proceedings should be aware that any document created electronically leaves a trail of potentially relevant admissible evidence, which can be questioned where a document's authenticity is put to proof.

In practical terms, where a matter in a dispute concerns contemporaneous evidence put forward in documentary evidence for example, and those documents are shown to have been created outside the dates relied upon, the documents can be questioned. The credibility of the witness can also be questioned where documents were habitually and frequently created at a much later date.

(b) Hard Copy Documents

Hard copy documents that have not been subject to scrutiny and verification from the original source should be questioned, particularly where that hard copy document is the single source of evidence and where there is no associated metadata for such documents. Where a question is raised about the authenticity of a hard copy document, the party producing the file should be put to proof, detailing how the document was created, where it was sourced from, and whether an original version exists. The original version of the document should be sought.

(c) Native Electronic Documents

The metadata of a native document (obtained by downloading and opening the document in native form) should match the metadata provided by the opposing side through the disclosure load-file. Where metadata does not match, and where there is a single source for this document, the party who has produced the document should be put to proof

(d) Images / jpg / TIF

PDF versions of documents should be ideally disclosed. Where image files are disclosed, and those images' metadata cannot be effectively verified, original source documents should be requested, together with any associated overlay metadata. Screenshots or images that cannot be proved should be challenged.

The role of forensic experts

Where accurate and accepted versions of documents whose authenticity are queried have not been forthcoming from the producing party, and where inaccuracies or inconsistencies exist within several produced documents, it is advisable that the party questioning the veracity of a document seek verification through the services of a forensic expert.

The duty of an expert witness is to help the court to achieve the overriding objective by giving opinion, which is objective and unbiased, in relation to matters within their expertise.

Cause and Effect Testing

Simply put, an expert will attempt to replicate the original document, using original source material. For example, where images are produced, an expert will scrutinise the language-style used, the software interface, as well as the document's text characters, to see if these are standard within the underlying software from which the document was allegedly sourced. Where something appears to look out of place, or where the interface and text style do not tally with the authentic version of the software, the document will be interrogated further. Variables such as bugs, software updates, or other potentials for alteration will be given due consideration. An expert opinion on the falsification of a document can be drawn where the identical devices and instances of software or other applications cannot replicate the content of the document produced.

Indicators of Manipulation

Spotting certain artefacts in varied types of data lead to further scrutiny of the produced document, however this will not draw a conclusive finding of falsification. As an example, photographs can show metadata that indicate they have been imported and opened in a tool like *Photos* on a Mac, however, this does not necessarily mean anything has been changed about the photo – the tool also acts as a viewer. If, however, the photograph appears to differ from what would be expected from the source data, cause and effect testing must be engaged.

Chain of Custody and Continuity of Data

When there are scenarios alleging different sets of the '*same*' documents or a disputed set of facts that are in some way papered, provenance becomes pronounced. A data forensic expert will want to collect and analyse, where possible, the true original piece of data underlying the produced document. For example, the document's metadata must be interrogated to identify whether it has been copied between computers, and if so, the author of the document must be identified. Further interrogation should be instigated to identify the device on which the original documents was created. Where messenger data, such as WhatsApp or Telegram messages are produced, the original phone devices should be sought to forensically image the data. Opinions and conclusions can always be formed, but the further one finds themselves from the original data, the less fortified these tend to be.

Peer Review

After a set of opinions and conclusions have been formed based on instruction and analysis, it is crucial that another (one or more) of data forensic subject matter experts review the expert's original findings to verify any inferences of falsification of evidence. This ensures avenues of inquiry are not overlooked, and also brings the power of the hive mind to the analysis at hand.

Conclusion

Where suspicion is raised, parties should be vigilant to interrogate suggestions of fraudulent evidence – although this may involve considerable time for practitioners and forensic experts, it goes to undermine the essence of an opponent's case, which may ultimately determine the case outcome.

Fiona is a Director in Fieldfisher's Dispute Resolution team. Fiona's practice predominantly focuses on UK High Court commercial litigation. Fiona also possesses qualifications in digital forensics and leads Fieldfisher's eDisclosure practice.

Dominic Tucker is an Associate Director at iDiscovery Solutions (iDS) where he leads digital forensic and eDisclosure exercises in support of litigation, arbitration and other contentious type matters and investigations.

Contact Us

Fiona Campbell
Director, Fieldfisher
Direct: +44 330 460 6620
Mobile: +44 7741 905675
Email: fiona.campbell@fieldfisher.com

Dominic Tucker
Associate Director, iDS Europe
Direct: 07818406834
UK: +44 (0)20 824 24130
US: +1.800.813.4832
Email: dtucker@idsinc.com