Browne Jacobson

The Post Office Horizon IT Scandal: How should organisations react when IT systems go wrong?

13 June 2024

This article was first published by the Society for Computers & Law

The Horizon Post Office Scandal has been described as one of the greatest miscarriages of justice in UK history and has become a pivotal case study on the subject of legal integrity. In addition to the more widely publicised issues associated with the Scandal, the matter also offers critical lessons in the governance and oversight of large-scale public contracts and IT systems management. This article focuses on the latter topic, and specifically, practical steps that organisations can take to mitigate against potential liability in situations where IT systems go wrong, whether that be due to system or human failure.

Background

The Horizon Post Office Scandal features heavily within public consciousness due to the nature of the Scandal, the long-running public inquiry, and various television dramatisations.

More than 900 subpostmasters were convicted of theft and false accounting after shortfalls in their branch accounts were discovered, and were wrongly prosecuted by Post Office and the Crown Prosecution Service. The Post Office itself took many of these cases to court, prosecuting 700 people between 1999 and 2015, whilst another 283 cases were brought by other bodies, including the Crown Prosecution Service.

One of the underlying causes of this injustice was Horizon, a digital accounting system provided by the IT multinational, Fujitsu and rolled out to thousands of Post Office branches in the early 2000s. Almost immediately after the installation, there were reports of unexplained accounting shortfalls. Under the previous paper-based system, it would have been relatively easy to review the accounts and find the cause for any shortfalls. The design and implementation of Horizon, and the reliance placed on the software within Post Office branches, meant the reason for the shortfalls could not be established. Whilst sub postmasters owned their own businesses (namely the local Post Office branches) they were agents for Post Office. As such, and in the first instance, explaining any accounting shortfalls would be the responsibility of the subpostmasters. Given the lack of clearly identifiable evidence, proving the shortfalls were attributable to IT system error was near impossible for many.

The evidential and factual fight battle subpostmasters engaged in was made more difficult by the fact that computer-generated evidence in English law cases is subject to a common law presumption that the computer system producing the evidential record was working properly at the material time and that the record is admissible as real evidence. This presumption is rebuttable if evidence to the contrary is adduced, in which case it is for the party seeking to produce the computer record to satisfy the court that the computer was working properly at the material time.

Ascertaining who is at fault when IT systems fail

The context described above is not unique to the Horizon Scandal, and the question of who is liable when IT systems go wrong will always be a factual one. When systems fail there will be a multitude of assessments that seek to establish (i) why the system failed; (ii) who was responsible for the failure; and (iii) who is liable for any losses that have been suffered as a result of the IT system failing. Difficulties in assessing these issues can lead to time consuming and expensive disputes. For instance, did the system fail because of an

underlying issue that was present at source (as was the case with the Horizon system), or was it because of the way in which the system was installed and implemented by the organisation or was the failure due to the way in which the system was operated by the employees and/or agent whose job it was to operate the IT system. Whilst a number of potential disputes between various different stakeholders might be triggered due to IT system failure, it is important to bear in mind that the nature of these disputes largely depends on the contractual relationships (i.e. between system provider (Fujitsu) and employer (Post Office) and between employer and employee/agents (sub postmasters)), what specifically goes wrong, and what is stated in the various liability and risk provisions of the relevant contracts.

Considerations for organisations when IT systems go wrong

One of the starkest aspects of the Horizon Scandal (as detailed in the public inquiry) was the way in which the concerns of sub postmasters were dismissed by the Post Office in favour of the reliance placed on the Horizon system.

Organisations should not default to, the presumption that computer systems producing evidential records were working properly at the material time. It is important to be alert to the fact that IT systems sometimes fail, and that failure could very easily be because of an inherent issue with the system itself as opposed to human error. In the case of a potential IT system failure, it is essential that organisations act quickly by investigating and documenting, to the extent that this is possible, the (i) the date on which the issue/s first arose; (ii) a description of the relevant issues; and (iii) any apparent and obvious causes of the system failure. Organisations should also consider instructing forensic experts at an early stage as this will provide a much clearer understanding of the cause of the failure and, importantly, ensure that the organisation is evidentially prepared for any litigation that might ensue. The early instruction of independent forensic experts can also mitigate against any potential bias and/or impartiality arguments being raised in relation to the investigation by other parties to the litigation.

A further lesson from the Horizon Scandal is that it is essential to ensure that the roles, responsibilities, expectations and allocation of risk between the various parties involved with the provision, installation and operation of the IT system are contractualised and defined in detail. When it came to Horizon, the Post Office could not say for certain where Fujitsu's role and responsibilities ended and theirs started, which resulted in reliance being placed on the default position that the Horizon software was infallible, and as such, the only logical explanation was that the sub postmasters were to blame.

In the event that an IT system fails, then it is likely that there will be multiple claims, with stakeholders seeking to recover their losses from the party next in the contractual chain. The claims will typically be for breach of contract arising from a failure to provide services in accordance with the express terms of the contract and/or with reasonable care and skill. Such claims may give rise to damages, termination rights and/or other contractual remedies specified in the contracts. Organisations should ensure that contractual arrangements with IT suppliers and employees/agents include specific warranties, indemnities and limitation provisions that are, to the extent that this is possible, tailored to the specific purpose of the IT system and should be based on standards that are clearly and objectively measurable.

Conclusion

The contractual issues referred to above are highly specific to the use to which the IT system will be put so contracting parties should seek to engage as early as possible with their stakeholders, consultants, lawyers and other experts to help them navigate this area.

As noted in the introduction to this article, the Horizon Scandal offers critical lessons in the governance and oversight of large-scale public contracts, and IT system management. Effective governance processes and audit trails are crucial for ensuring data oversight and for exposing discrepancies and inconsistencies in IT systems as early as possible.

From a corporate governance perspective, it appears surprising that the Horizon narrative was not challenged at a board level. As the Horizon Scandal demonstrates, in situations where IT systems fail and litigation ensues, directors could potentially find themselves to be in breach of section 172 of the Companies Act 2006, which places on company directors a legal "duty to promote the success of the company", and/or the UK Corporate Governance Code (UKCGC) 2024 which notes that "all directors must act with integrity, lead by example and promote the desired culture". To mitigate against this, and to improve trust and transparency, organisations should establish internal guidelines and policies, and implement an appropriate governance framework to address the specific risks associated with IT system failure.

Given the close scrutiny the Horizon Scandal has attracted, we anticipate that the courts may re-evaluate the common law presumption cited above. Notwithstanding the fact that it is common for IT systems/software to fail for all manner of reasons, the rebuttable presumption will likely become increasingly unsuitable in a world in which Artificial Intelligence use is becoming ever-present. The inherent complexity and uncertainty associated with AI means that, in most cases, it will be virtually impossible to ascertain why the AI failed and who is to blame – was it the data used by the AI developer to train the AI tool or was it because the training methodology used by the AI developer was flawed or inadequate, or did the IT supplier fail to exercise sufficient oversight over the outputs that the AI tool produced before submitting outputs to the end user?

How the courts re-evaluate the common law presumption on computer-generated evidence could easily form the basis of a separate article. For present purposes we would suggest that there needs to be, at the very least, clear recognition that errors do arise in evidence from IT systems. One possible solution would be to shift the burden of proof onto the organisations seeking to rely on computer generated evidence and stipulate that early disclosure (either in the pre-action phase or during pleadings) of documents and evidence be provided to allow the court to consider and assess, to the extent that it can, whether the computer-generated evidence is reliable and admissible.

Key contacts

Henrietta Scott

Head of Marketing

PRTeam@brownejacobson.com

+44 (0)330 045 2299

Andrew Woolsey

Associate

Andrew.Woolsey@brownejacobson.com

+44 (0)330 045 2702

Related expertise

Commercial contracts for retail

Commercial dispute resolution

Commercial law

Information law

Public contracts, projects and funding