# Merseyside law firm fined £60,000 for data breach following 2022 cyber attack



Merseyside-based law firm DPP Law Ltd has been fined £60,000 by the Information Commissioner’s Office (ICO) following a cyber attack in 2022 that led to a significant personal data breach. The firm, which specialises in criminal law and cases involving actions against the police, experienced unauthorised access to its network during the incident, resulting in the theft of over 32GB of data.

The breach was initially detected not by the firm itself but after the National Crime Agency (NCA) alerted DPP Law that some of its clients’ information had been posted on the dark web. This prompted a deeper investigation into the full extent of the attack. According to the ICO, DPP Law failed to report the breach within the legally required 72-hour period and only notified the regulator 43 days after becoming aware of the issue. The firm had not regarded the loss of access to personal data as constituting a personal data breach at first.

Andy Curry, director of enforcement and investigations at the ICO, stated: “Our investigation revealed lapses in DPP’s security practices that left information vulnerable to unauthorised access. In publicising the errors which led to this cyber attack, we are once again highlighting the need for all organisations to continually assess their cybersecurity frameworks and act responsibly in putting in place robust measures to prevent similar incidents.” He further emphasised that data protection is a legal obligation, and failure to safeguard personal information carries serious consequences.

The attack was triggered when DPP’s email server ceased functioning, and employees lost access to their IT network. An external IT supplier initially diagnosed the issue as ransomware, despite there being no ransom demand. It was later found that a laptop used by an end-user had been compromised a day prior to the network disruption. During the following week, DPP examined firewall and server logs and initially assumed no data had been extracted. However, the NCA subsequently informed the firm that three folders containing various documents, including court bundles, PDFs, photos, videos, and police bodycam footage related to clients and expert witnesses, had been published online.

Further investigation revealed that the breach was executed through an old case management system's administrator account, which had been kept active for access purposes but possessed full administrator rights. This account was rarely used and allowed attackers entry via a remote desktop machine. The system had been maintained according to the Solicitors Regulation Authority’s guidelines. Nonetheless, DPP Law did not carry out a risk assessment concerning this account, reportedly following advice from the company that initially set up the system.

Following the attack, DPP Law undertook significant changes, moving its case management, accounts, and email systems to a new hosting environment. It also sent notifications to all affected individuals. The firm acknowledged it was heavily reliant on third-party IT contractors and had a limited internal IT function, which they described as “unsophisticated.” Although steps have since been implemented to enhance cybersecurity, the ICO clarified that these measures were not considered mitigating factors because they should have been in place prior to the incident.

DPP Law has publicly disagreed with the ICO’s conclusions and confirmed plans to appeal the fine. The firm emphasised its cooperation during the investigation and highlighted its existing security certifications. In a statement, the law firm said: “DPP Law holds the Law Society quality standard, Lexcel, and is Cyber Essentials certified. This demonstrates our commitment to robust standards in both legal practice management (Lexcel) and cybersecurity (Cyber Essentials). These independent certifications are intended to assure clients and stakeholders of our adherence to best practices.”

Since the breach, DPP Law has reportedly received five potential professional negligence claims, including from three individuals whose personal data was stolen. These claimants allege that the data theft caused them distress, shock, and anxiety.

The Law Gazette is reporting the developments surrounding DPP Law Ltd’s cyberattack and subsequent fine from the ICO.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.dataguidance.com/news/uk-ico-fines-dpp-law-ltd-ps60000-over-data-security> - This URL supports the claim that DPP Law Ltd was fined £60,000 by the ICO for data security failures. It provides details about the fine and the factors leading to it.
* <https://ico.org.uk/action-weve-taken/enforcement/2025/04/dpp-law-ltd/> - This URL from the Information Commissioner's Office corroborates the enforcement action taken against DPP Law Ltd and provides official details about the investigation and fine.
* <https://therecord.media/uk-law-firm-fined-ico-ransomware-sensitive-data-breached> - This article supports the information that the breach involved the publication of sensitive data by cybercriminals and that DPP Law was fined for the security lapses.
* <https://www.mlex.com/mlex/technology/articles/2326126/dpp-law-fined-in-uk-for-breach-of-clients-data-after-cyberattack> - This URL provides confirmation of the cyberattack leading to a breach of clients' data and explains the ICO's role in fining DPP Law.
* <https://www.nca.gov.uk/> - The URL for the National Crime Agency supports the claim that it was the NCA that informed DPP Law of data being posted on the dark web.