LEXOLOGY

Register now for your free, tailored, daily legal newsfeed service.

Register

Find out more about Lexology or get in touch by visiting our **About** page.

From Boardrooms to Courtrooms: Responding to Employee Data Theft

Trilegal

India | October 14 2025

Introduction

In today's corporate battlefield, data is the new oil - and leakage has unfortunately, become rampant. As competition intensifies, the line between fair and foul play blurs. Employees are often caught in a catch-22 situation, torn between loyalty, ambition, and lucrative opportunities. In this climate, access to client lists, trade secrets, pricing strategies, drawings and proprietary technology is not only an asset but also a dangerous temptation - one that makes walking away with critical information hard to resist.

Data theft is no longer rare and erodes a company's competitive edge and reputation[1]. Often, such theft surfaces through whistleblower complaints, internal investigations, or security alerts. We see in most situations, management scrambles to contain the damage. Clear and established streamline processes and trained legal teams give companies the edge to respond swiftly and effectively[2]. In fact, data theft extends beyond boardrooms – spilling into courtrooms, leaving companies with a dual challenge: responding now and preparing for the future.

The First Response: Unfortunately, is Reactive!

When employee data theft is suspected or confirmed, companies must act swiftly and launch an internal investigation while preserving records and devices[3]. Involving IT, forensic, and legal experts at the outset helps ensure evidence is secured[4]. Issuance of legal hold is key to preserving evidence and also engaging media experts to control the narrative. Such evidence may include emails, chat logs, print records, external storage devices, or workplace messaging exchanges, which supports the investigation and becomes critical in seeking protective orders from Indian courts. Once evidence is secured, companies need to assess the damage and analyse findings that may warrant legal action. The need of the hour is for corporates to contain the loss and simultaneously ensure that business runs as usual.

Civil Remedies in Action: How Courts Protect Confidential Information

Post completion of the investigation, corporates face the major dilemma, pursuing legal route or focussing on business. However, the real test is what qualifies as '*confidential information*' and whether such leakage can be enforced in Indian courts. Not every spreadsheet deserves a lock and key - only a company's lifeblood does.

In December 2024, the Delhi High Court, in ***Cigma Events Private Limited v. Deepak Gupta and Ors.[5]s***, underscored that labelling existing business information as confidential or a trade secret is insufficient. The case involved allegations against former employees of a company who were accused of starting a competing business and attempting to poach the clients of their former employer. The central issue, before the Delhi High Court, was

analysing whether the client list of a business can be deemed proprietary information or a trade secret deserving legal protection through an injunction, particularly when it concerns employees who have acquired knowledge of the company's clients during their employment. The Delhi High Court, answering in the negative and denying the injunction, categorically held that a client list, by itself, is not automatically protected as confidential information simply by virtue of its existence. To be considered a trade secret or confidential information, it must possess economic or business value that requires safeguarding against competitors. The emphasis was on need to distinguish between information that is generally known or accessible in the public domain and information that is truly confidential, which alone merits the protection of an injunction.

Indian courts have taken a zero-tolerance stance on employee data theft, recognising its gravity. Common reliefs include (a) *ex-parte ad-interim* injunctions against employees[6]; (b) appointment of forensic experts and court commissioners to secure data and safeguard the Company's interests[7]; and (c) retention of electronic devices at early stages to preserve data/ evidence[8].

In yet another decision in December 2024, the Bombay High Court in ***H and K Rolling Mill Engineers Private Limited and another v. Dipak Balshiram Kale and Ors***[9] pertaining to a case involving allegations that former employees had misappropriated large volumes of sensitive material. The Bombay High Court, in its order, observed that the company had supported its claim with substantial evidence, including receipts showing proxy sales through a relative's entity, correspondence and screenshots of offers, as well as a website printout advertising an identical component. The Court further noted that there was evidence of poaching attempts, with emails and WhatsApp messages indicating approaches made to current employees. In light of this strong *prima facie* case, the Bombay High Court passed sweeping ad-interim orders, directing the appointment of a Court Receiver, assisted by a third-party forensic expert (at the company's cost), and vested with extensive powers to seize and take custody of the employees' personal devices (computers, laptops, storage drives, and cloud accounts, along with passwords). The Receiver was directed to prepare an inventory of the confidential information, trace its circulation, and create mirror copies of all relevant electronic data, ensuring that only offending material was copied, while personal data remained undisturbed. To secure compliance, the Receiver was authorised to break open locked premises with police assistance, if necessary.

In fact, the Delhi High Court, in ***HT Process Controls Private Limited v. Ankur Gupta and others***[10], noted the importance of early preservation of evidence in cases involving misappropriation of confidential information. The Delhi High Court observed that on inspection of a company-issued laptop revealed that, just before resigning, an employee had forwarded confidential documents from his official email account to his personal account. This was viewed as a clear evidence of misappropriation, and, at interim stage, protective reliefs were directed. The above series of decisions illustrate a clear judicial trend: courts are prepared to act swiftly and decisively where companies present credible evidence of data theft. However, the burden of demonstrating confidentiality and securing such proof continues to rest squarely on the company.

The Criminal Route

Companies in addition to civil remedies, may pursue criminal action by filing complaints with the relevant authorities.[11]. Such proceedings can expose former employees to a range of criminal liabilities. Under the Bharatiya Nyaya Sanhita, 2023, relevant provisions include Section 238 (causing disappearance of evidence or giving false information to screen an offender), Section 241 (destruction of electronic records to prevent their production as evidence), Section 303 (theft), Section 317 (stolen property), and Section 318 (cheating). Under the Information Technology Act, 2000, key provisions include Section 43 (penalty and compensation for damage to computer systems), Section 65 (tampering with computer source documents), and Section 66 (computer-related offences). However, companies must be mindful that criminal law carries a higher evidentiary threshold than civil proceedings. Accused employees often challenge the very basis of complaints through quashing

petitions. Recently, the Karnataka High Court quashed proceedings against former employees accused of client data theft, breach of trust, and IT Act violations, holding that such disputes were more appropriately addressed through civil remedies such as injunctions and restraining orders[12]. Courts have held that justice system cannot be used as a substitute for recovery of money, unless the facts are glaring and disclose a clear offence[13].

Conclusion*: *Building a Firewall against Data Theft

Prevention is better than cure—and it is not any more true than in the context of employee data theft. Indian courts have shown readiness to protect companies by granting injunctions, appointing commissioners, and even directing seizure of devices. Yet litigation, while effective, is inevitably reactive. The real strength lies in preparedness: preventing breaches before they occur, responding decisively when they do, and learning from the aftermath. A corporate hygiene checklist for companies to act when faced with such scenarios[14]:

1. **Preventive Measures** –(i) Strong safeguards to protect sensitive information; (ii) Limiting access strictly to only necessary resources; (III) Ensuring execution of confidentiality agreements and employment contracts and (iv) Conducting periodic review through audits.
2. **Crisp and clear contracts** – Employment contracts, NDAs, and policies should clearly define what constitutes confidential, how it can be used, and the consequences of misuse.
3. **Exit Protocols** – (I) Immediate cut-off access to company devices; (ii) Recover company devices, and obtain written undertakings that no confidential information has been taken or retained.
4. **Awareness and Training** – A culture of confidentiality is as important as legal safeguards. Regular training and reminders about ethical duties and consequences of misuse help prevent lapses.
5. **Reporting Channels** – Encourage whistleblowers and create safe, anonymous routes for reporting suspicious activity before it escalates.
6. **Incident Readiness** – Even with the best safeguards, breaches may still occur. Maintain a response team —legal, HR, IT, and senior management—to act immediately: investigate, preserve evidence, restrict further misuse, and ensure business continuity.
7. **External Support** –Lawyers and forensic experts to be kept on standby to initiate immediate action within hours if needed.
8. **Mitigation and Redressal**– Once a breach is contained, review what went wrong, strengthen internal processes, and update training and policies. Every incident should become a learning opportunity.

The corporates cannot rely on courts alone in today's age - proactive mitigation, cultural awareness, decisive response, and legal recourse all go hand in hand to prevent such leakages. The fight against employee data theft begins in the boardroom - with strategy, culture, and controls - and often ends in the courtroom, with enforcement action, in the absence of proper controls.

Trilegal - Payel Chatterjee, Shuchita Choudhry and Pranay Tuteja

*If you would like to learn more about our firm and areas of expertise, please feel free to drop in your queries **here**.*

Interested in contributing?

Get closer to winning business faster with Lexology's complete suite of dynamic products designed to help you unlock new opportunities with our highly engaged audience of legal professionals looking for answers.

Learn more