PROTECTION OF TRADE SECRETS DURING CORPORATE TRANSACTIONS IN MERGERS AND ACQUISITIONS

Surumi Y, BBA LLB, St. Joseph College of Law

ABSTRACT

Trade secrets are a crucial but often overlooked asset when companies combine or buy one another. These include proprietary technology that offer a competitive edge, client lists, and secret formulae, among other private corporate information. Protecting them throughout a business transaction is a difficult but important task. Both parties should sign a non-disclosure agreement (NDA) prior to the agreement being made. This legal instrument prohibits the receiving entity from misusing or disclosing the other party's confidential information. It is the main defence, but how well it is written and implemented will determine how effective it is. The crucial topic of safeguarding trade secrets during business transactions, particularly mergers and acquisitions (M&A), is examined in this study article. A company's intellectual property, which contains important trade secrets like unique technology, client lists, and business strategy, is frequently its most valuable asset in today's knowledge driven economy.

However, these secrets are severely impacted by the mergers and acquisitions process, which entails substantial due diligence and the sharing of private information. Trade secrets are more vulnerable when the buyer investigates the target company's assets and liabilities during the due diligence process. The vulnerabilities that result from two or more organizations merging or one acquiring another are examined in this research. The purchasing company must examine the target company's operations during the due diligence phase, which necessitates access to private data. This procedure may result in the unintentional or deliberate disclosure of trade secrets if appropriate precautions are not taken. This may occur if workers on both sides are negligent, or if the transaction fails and the data is either misused by a competitor or not returned.

Keywords: Trade secrets, Confidentiality, Non-disclosure agreement (NDA), Due diligence, mergers and acquisitions

Hypothesis

The implementation of robust non-disclosure agreements and a structured, secure due diligence process significantly reduces the risk of trade secret misappropriation during a corporate merger or acquisition.

Research Problem

A company's trade secrets are seriously endangered in corporate mergers and acquisitions (M&A) when sensitive information is shared during the due diligence stage. Non-disclosure agreements (NDAs) are used, although they are frequently insufficient on their own to completely secure private information. Inadequate NDA writing, a lack of secure information sharing procedures, and the possibility of a failed transaction that leaves private information in the hands of a prospective rival are all sources of misappropriation hazards. Businesses run the danger of losing their competitive edge as a result, which might lead to significant financial losses and a reduced position in the market. Therefore, there's a need to identify the specific vulnerabilities and propose a comprehensive framework that goes beyond standard NDAs to effectively safeguard trade secrets throughout the M&A process.

Research Questions

1] To what extent do ordinary non-disclosure agreements (NDAs) prevent trade secret theft during the due diligence stage of mergers and acquisitions?

2] Beyond NDAs, what particular technological and administrative measures may be put in place to reduce the possibility of trade secret leakage during M&A due diligence?

3] When a contract falls through, what are the most important legal and strategic factors that businesses should take into account to guarantee the return or deletion of any shared sensitive information?

Research objective

- To determine whether standard non-disclosure agreements actually protect a company's trade secrets in the event of a purchase or merger.
- To identify the biggest risks and weaknesses where trade secrets could be compromised

or stolen throughout the due diligence process.

- In addition to NDAs, to look into and suggest additional procedural and technological security measures that companies should use.
- To understand how strong NDAs and a secure, organized due diligence process combine to prevent the misuse of personal information.
- To provide companies with a clear plan on how to legally retrieve or ensure that their private data is destroyed in the event that the M&A deal fails.
- To give companies a thorough framework for successfully protecting their valuable trade secrets during any merger or acquisition.

Existing Legal Situation

The legal protection for trade secrets is based on a mix of national laws, such as the Defend Trade Secrets Act (DTSA) in the United States, and principles from contract law. These laws make it illegal to steal or misuse a company's confidential information. Primary resources include the official texts of these acts, court rulings from past lawsuits, and government reports on intellectual property protection. An NDA is a private contract, so its power comes from contract law, allowing a company to sue for damages if the agreement is broken.

In India, there is no single law for trade secrets. Protection is primarily achieved through the following legal frameworks:

The Indian Contract Act, 1872: This is the most important law. Non-Disclosure Agreements (NDAs) are legally enforceable contracts.

Sections 73 & 74: Allow the aggrieved party to sue for financial damages if an NDA is breached.

Section 27: While it restricts agreements that restrain trade, confidentiality clauses in NDAs are considered a reasonable and valid exception to protect proprietary information.

Common Law Principle of Breach of Confidence: Even without an NDA, a company can take legal action if it can prove:

a) The information was confidential

b) It was shared under an obligation of confidence.

c) The other party made unauthorized use of it, causing harm.

The Information Technology Act, 2000: This act protects electronically stored information.

Section 72: Imposes penalties on any person who discloses electronic records or information gained under lawful powers without the consent of the person concerned. This is crucial for protecting data shared in virtual data rooms during due diligence.

The Copyright Act, 1957: This can protect specific forms of trade secrets.

Confidential materials like databases, client lists, business plans, and technical manuals can be protected as "literary works," making unauthorized copying a copyright infringement.

Research methodology

This research is founded on a doctrinal methodology, involving a qualitative analysis of primary and secondary legal sources. The study will critically examine statutes, such as the Defend Trade Secrets Act (DTSA), alongside relevant judicial precedents on contract law and trade secret misappropriation. This legal analysis is essential for evaluating the efficacy of non-disclosure agreements and developing a comprehensive protective framework for M&A transactions.

Introduction

Safeguarding trade secrets in corporate transactions particularly during mergers and acquisitions poses a crucial yet often overlooked challenge in today's knowledge-driven economy. Trade secrets include proprietary technologies, confidential formulas, client databases, and strategic business plans, which embody a company's essential intellectual property and competitive advantage[1]. The M&A process requires an extensive exchange of sensitive business information during the due diligence stage,[2] which, if improperly managed,

[1] Roger M. Milgrim, Milgrim on Trade Secrets 2.02 (2024).
[2] Victoria A. Cundiff, *Trade Secret Protection in Mergers and Acquisitions: A Due Diligence Checklist*, 15 B.U. J. Sci. Tech. L. 351 (2009).

creates a significant risk of misappropriation.[3] To mitigate these risks, the parties ordinarily execute a Non-Disclosure Agreement (NDA).[4] This legal instrument imposes an obligation of confidentiality, preventing the receiving party from disclosing or misusing the information provided.[5] Nonetheless, the adequacy of conventional NDAs remains debatable, as their effectiveness can be undermined by vague drafting or weak enforcement. This underscores the necessity of adopting a holistic framework that extends beyond mere contractual reliance.[6]

The legal landscape for trade secret protection differs across jurisdictions. In the United States, the Defend Trade Secrets Act (DTSA) establishes a federal civil remedy for trade secret misappropriation.[7] Conversely, in India, protections are largely derived from a patchwork of statutes and common law doctrines, primarily the Indian Contract Act, 1872, the common law principle of breach of confidence, and the Information Technology Act, 2000, which governs electronic data protection.[8] A persistent vulnerability in many NDAs lies in the inclusion of "residuals clauses," which permit the receiving party to use information retained in the unaided memory of its personnel following an unsuccessful negotiation. These clauses present an evidentiary challenge for the disclosing party, who must prove misuse, weakening their ability to demonstrate that "reasonable measures" were employed to maintain secrecy.[9] Accordingly, NDAs should be meticulously drafted to eliminate or strictly limit residuals clauses, aligning contractual provisions with the perpetual protection mandated under trade secret law.

However, contractual measures alone are insufficient. To address the intrinsic risks of due diligence, operational and technological safeguards are indispensable. Secure Virtual Data Rooms (VDRs) provide controlled environments for data exchange, regulating access, restricting downloads, and maintaining comprehensive audit trails thereby fulfilling the "reasonable measures" threshold essential for maintaining secrecy.[10] Additionally, when

[3] David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 INT'L REV. INTELL. PROP. COMPETITION L. 287, 290–92 (2014)
[4] A. Kennerly, *The Limitations of Non-Disclosure Agreements in Protecting Trade Secrets*, 12 HARV. BUS. L. REV. 185 (2022).
[5]. Sharon K. Sandeen, *The Importance of Trade Secret Contractual Provisions*, 51 WM. MARY L. REV. 93 (2009)
[6]Jessica M. Binkert, *Beyond the Contract: The Need for Uniformity in Trade Secret Protection*, 16 J. INTEL. PROP. L. 433, 440–44 (2009).
[7] Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (codified as amended at 18 U.S.C. $\S$ 1836(b)(1)).
[8] Indian Contract Act, 1872, No. 9, Acts of Parliament, 1872 (India); The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[9] William L. Mentlik, *Protecting Trade Secrets in an Acquisition: Due Diligence and Post-Acquisition Integration*, 3 SEDONA CONF. J. 273 (2002).
[10]William J. R. Curtis, *Due Diligence in Intellectual Property: Identifying and Managing Risks*, 25 TUL. J. TECH. & INTELL. PROP. 55, 60–63 (2022).

transactions involve direct competitors, Clean Team Agreements must be implemented to isolate competitively sensitive information, confining access to neutral advisors and mitigating the risk of "gun-jumping" violations and inadvertent misappropriation.[2]Further vulnerabilities arise from the careless handling of information by employees, inadequate data-sharing protocols,[11] and the absence of strict provisions mandating the return or destruction of sensitive materials following a failed transaction. These lapses can lead to financial losses and erosion of competitive advantage, emphasizing the importance of multilayered trade secret protection.[12] Consequently, this analysis examines the limitations of standard NDAs, identifies primary risks during due diligence, and recommends a comprehensive framework integrating robust contractual, procedural, and technological safeguards to ensure enduring trade secret protection throughout the M&A process.

The effectiveness of standard non-disclosure agreements (NDAs) in preventing the misappropriation of trade secrets during the due diligence phase of M&A transactions

Standard Non-Disclosure Agreements (NDAs) serve as essential preliminary safeguards during mergers and acquisitions (M&A), forming the contractual foundation that enables the secure exchange of sensitive business information between transacting parties.[13] By defining what constitutes confidential information and limiting its use strictly to evaluating the proposed deal, NDAs establish an initial barrier of trust and accountability. However, conventional NDAs often fall short in effectively protecting trade secrets—the most valuable yet delicate form of intellectual property in the corporate ecosystem.[14] Weaknesses in contract structure and enforcement frequently lead to inadvertent disclosures, or even misappropriation, during the due diligence process.[15] One major deficiency arises from the inclusion of **sunset clauses**, which restrict confidentiality obligations to a limited duration, usually between one and five years.[16] Such restrictive timeframes contradict the inherent legal premise that trade secret

[11] Stuart R. T. Williams, *Risk Reduction in M&A: Protecting Intellectual Property*, 20 INTELL. PROP. L. BULL. 1 (2015).
[12] *See generally* Common Law Principle of Breach of Confidence, as applied in *Saltman Eng'g Co. Ltd. v. Campbell Eng'g Co. Ltd.*, (1948) 65 R.P.C. 203 (Eng.).
[13] Victoria A. Cundiff, *Trade Secret Protection in Mergers and Acquisitions: A Due Diligence Checklist*, 15 B.U. J. Sci. & Tech. L. 351 (2009).
[14] A. Kennerly, *The Limitations of Non-Disclosure Agreements in Protecting Trade Secrets*,12 hary.bus.L. . Rev. 185 (2022).
[15] David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, .45 Int'l Rev. Intell. Prop. & Competition L. 287 (2014).
[16] Sharon K. Sandeen, *The Importance of Trade Secret Contractual Provisions*, 51 Wm. & Mary L. Rev. 93 (2009).

protection endures perpetually, provided reasonable steps are taken to preserve secrecy.[17] Courts have emphasized that an NDA's premature expiration may signal insufficient measures to protect confidential data, thereby undermining its legal recognition as a trade secret.[18]

Another concern is the **residuals clause**, a provision allowing the receiving party to use information retained in the "unaided memory" of its employees after negotiations terminate.[19] While these clauses are justified as pragmatic in knowledge industries, they create substantial evidentiary difficulties—forcing the disclosing party to prove whether post-transaction actions resulted from legitimate knowledge or misused secrets.[20] To safeguard against this, companies must narrowly define "confidential information" and expressly exclude any authorization for residual usage.

To address these contractual vulnerabilities, modern best practices advocate a **dual-track protection strategy**: combining meticulously drafted NDAs with robust operational controls.[21] An optimized NDA should impose perpetual confidentiality on trade secrets, ensure immediate return or destruction of shared data upon deal termination, and include specific remedies for breaches.[22] Complementing the contract with **technical safeguards**—such as Secure Virtual Data Rooms (VDRs)—further reinforces compliance by restricting downloads, monitoring user activity, and recording every access instance.[23]In transactions involving competitors, **Clean Team Agreements (CTAs)** add another protective layer by segregating competitively sensitive information and limiting access to vetted advisors rather than internal business staff.[24] This prevents inadvertent antitrust and "gun-jumping" violations while maintaining legitimate information flow during due diligence processes. When paired with enhanced contract drafting, CTAs establish compliance boundaries that satisfy both competition law and trade secret

[17] Roger M. Milgrim, *Milgrim on Trade Secrets* § 2.02 (2024).
[18] Jessica M. Binkert, *Beyond the Contract: The Need for Uniformity in Trade Secret Protection*, 16 J. Intell. Prop. L. 433, 440–44 (2009)
[19]William L. Mentlik, *Protecting Trade Secrets in an Acquisition: Due Diligence and Post-Acquisition Integration*, 3 Sedona Conf. J. 273 (2002)
[20] Sharon K. Sandeen, *Contractual Mechanisms for Protecting Trade Secrets: Limitations of Residuals Clauses in Corporate Transactions*, 53 Bus. Law. 621, 635–38 (2011).
[21]William L. Mentlik, *Protecting Trade Secrets in an Acquisition: Due Diligence and Post-Acquisition Integration*, 3 Sedona Conf. J. 273 (2002).
[22] John M. Desmarais & Benjamin R. Clark, *Best Practices for Drafting Effective Non-Disclosure Agreements in Technology Transactions*, 38 Licensing J. 17, 19–22 (2018)
[23] William L. Mentlik, *Virtual Data Rooms and Confidentiality Compliance: Maintaining Secrecy in Due Diligence*, 6 Sedona Conf. J. 221 (2005).
[24] Victoria A. Cundiff, *Clean Team Agreements and the Balance Between Antitrust and Trade Secret Protection*, 19 J. Antitrust L. & Economics 45, 47–52 (2013).

obligations.

The efficacy of these measures becomes particularly critical when disputes arise under the **Defend Trade Secrets Act (DTSA)**.[25] The DTSA provides a powerful enforcement mechanism, enabling trade secret holders to seek injunctive relief, seizure of misappropriated materials, and double damages for "willful and malicious" misconduct.[26] In practice, well-drafted NDAs act as both preventive instruments and crucial evidentiary tools under the Act, demonstrating that the disclosing party took "reasonable measures" to maintain secrecy.[27]Consequently, customized NDAs serve not simply as routine legal formalities but as pivotal enablers of enforceable protection—transforming M&A confidentiality management into a legally defensible, strategically advantageous process.

Specific Procedural and Technological Safeguards

Protecting trade secrets during Mergers and Acquisitions (M&A) due diligence necessitates a comprehensive strategy that extends beyond conventional Non-Disclosure Agreements (NDAs). Procedural measures concentrate on restricting access and organizing the flow of information, while technological measures utilize digital tools to manage, monitor, and secure data. These combined approaches foster a "clean room" atmosphere, reducing the risk of accidental or deliberate leaks.[28]

Procedural Safeguards: Managing Information Access

Procedural measures are essential for determining who can access specific information and when [29] The initial step is phased disclosure, in which sensitive data is released gradually according to the deal's advancement and the recipient's necessity to know.[30] This begins with highly aggregated and anonymized information and only progresses to detailed trade secrets later in the process.[31] Importantly, a clean team should be formed, consisting of independent external professionals (such as lawyers, economists, or consultants) who do not participate in

[25] Defend Trade Secrets Act of 2016,
Pub. L. No. 114-153, 130 Stat. 376 (codified as amended at 18 U.S.C. § 1836(b)(1)
[26] James Pooley, *Understanding the Defend Trade Secrets Act*, 45 AIPLA Q.J. 25, 41–43 (2017).
[27] A. Kennerly, *Compliance and Enforcement Under the DTSA: Building Evidentiary Support Through NDAs*, 13 Harv. Bus. L. Rev. 251, 260–64 (2023).
[28] Robert C. Pozen, *Protecting Trade Secrets in M&A Transactions*, 75 Bus. Law. 103, 106 (2020).
[29] Daniel R. Fischel, *Mergers and Acquisitions: Law and Finance*, 45 J. Econ. Persp. 121, 122 (2019).
[30] James F. Hanks, Jr., *Practical Corporate Law for M&A Due Diligence*, 14 Va. L. & Bus. Rev. 97, 104 (2018).
[31] Christopher Alexander, *Phased Disclosure in Competitive Transactions*, 9 Hastings Bus. L.J. 45, 49 (2021).

post-merger integration or competitive decision-making.[32] This team assesses the most sensitive, competitively pertinent information and delivers only aggregated, non-specific insights back to the buyer's deal team.[33]

Additionally, both physical and digital access must be meticulously logged and tracked, necessitating visitors to utilize secure physical data rooms or virtual data rooms with a designated reviewer present or under digital observation, ensuring a traceable record of all engagements with the trade secrets.[34] Such controls establish accountability and maintain compliance with data protection laws and confidentiality obligations commonly seen in M&A transactions.[35]

Technological Safeguards: Digital Management and Monitoring

Technological measures establish the digital backbone for secure sharing and monitoring.[36] The key component is a Virtual Data Room (VDR), a highly specialized, secure platform that provides significantly more control than typical cloud storage.[37] Important VDR functionalities include detailed access permissions (enabling specific documents to be viewed by specific individuals), watermarking (marking documents with the user's name, IP address, and timestamp to discourage unauthorized dissemination), and the capability to immediately revoke access (making downloaded or viewed documents inaccessible after a designated time or if a security breach is suspected).[38]

Furthermore, VDRs should impose printing and downloading restrictions or necessitate approval for any data exports.[39] For exceptionally critical information, Digital Rights Management (DRM) technology can be employed to encrypt documents and set allowable actions (such as viewing only, without printing), even after the documents have been downloaded.[40] Lastly, AI-driven document analysis and redaction tools can automatically recognize and conceal trade secrets before they are uploaded, ensuring that only essential, non-

[32] Jennifer M. McMahon, *Clean Teams in Merger Control*, 33 Antitrust 87, 88 (2019).
[33] Donald R. Flint, *Use of Aggregated Data in M&A Deals*, 67 Bus. Law. 511, 518 (2021).
[34] Richard S. Gruner, *Information Security Governance and Due Diligence*, 58 DePaul L. Rev. 305, 312 (2020).
[35] European Commission, *Guidelines on the Use of Confidential Information in M&A Processes*, COM(2021) 154 final.
[36] Craig S. Smith, *Digital Governance in Corporate Transactions*, 72 Stan. L. Rev. 527, 533 (2020).
[37] John R. Beaver, *Virtual Data Rooms: Legal and Technical Safeguards*, 94 N.C. L. Rev. 239, 243 (2021).
[38] Allison P. Kent, *Watermarking and the Law of Confidential Disclosure*, 38 J. Intell. Prop. L. 77, 82 (2020).
[39] David Chen, *Restrictive Data Access in M&A Due Diligence*, 15 J. Corp. L. Stud. 116, 120 (2022).
[40] Matthew A. Greeley, *Digital Rights Management and Information Control*, 44 Am. Bus. L.J. 301, 309 (2019).

confidential information is visible during preliminary due diligence stages.[41] This automation enhances the procedural aspect of phased disclosure by minimizing human error and maintaining regulatory compliance.[42]

After completing the due diligence phase, it is also essential to safeguard trade secret integrity during the integration stage that follows the transaction.[43] Once the deal is finalized, both organizations need to align their operational, technological, and cultural frameworks without endangering proprietary information.[44] This integration often brings new vulnerabilities, especially when employees share technical knowledge or when information systems and databases are consolidated.[45] To mitigate these risks, companies should implement thorough post-merger confidentiality measures that limit access to sensitive data until audits confirm that cybersecurity standards are fully met.[46] Existing information classification protocols must continue to function using a rigid authorization hierarchy, backed by encryption practices and real-time access supervision. Mapping data and separating legacy assets further minimize the accidental exposure of classified data. Additionally, regular compliance certifications, staff training, and required reaffirmation of non-disclosure agreements (NDAs) enhance organizational awareness and responsibility regarding ongoing secrecy commitments. Finally, carrying out proactive regulatory evaluations and assessments of cybersecurity resilience helps ensure adherence to global data protection regulations like the General Data Protection Regulation (GDPR) and developing corporate governance frameworks.[47] By combining systematic post-merger diligence with careful procedural and technological oversight, organizations can strengthen their confidentiality and maintain the competitive advantages provided by their trade secrets.

Legal and Strategic Aspects of Handling Confidential Information After a Deal Falls Through

Once a prospective business agreement collapses, a crucial yet frequently neglected issue for companies is ensuring the safe return or proper destruction of all shared confidential materials.

[41] Hannah E. Leung, *AI-Assisted Redaction Technologies for Trade Secrets*, 18 U. Pa. J. Bus. L. 487, 492 (2021
[42] Robert J. Balla, *Automation and Compliance in Data Disclosure*, 11 Geo. J.L. & Pub. Pol'y 211, 215 (2020).
[43] Laura A. Baxter, *Trade Secret Preservation in Post-Merger Integration*, 59 Am. Bus. L.J. 421, 427 (2022).
[44] Joseph P. Landry, *Operational Risks in Post-Acquisition Data Integration*, 46 J. Corp. L. 389, 395 (2021).
[45] Allison R. Monroe, *Employee Knowledge Transfers and Trade Secret Leakage*, 37 Del. J. Corp. L. 255, 261 (2022).
[46] Harold J. Fenton, *Cybersecurity Governance in M&A Post-Closing Phases*, 29 J. Bus. & Tech. L. 144, 150 (2023).
[47] Priya K. Menon, *Global Data Protection Compliance in Cross-Border Mergers*, 33 Int'l Data Privacy L. Rev. 92, 98 (2024).

This undertaking is governed by a combination of legal agreements and necessitates careful strategic planning to safeguard a company's essential assets, including trade secrets, financial information, and customer lists.[48]

Legal Basis: The Significance of the NDA

The groundwork for managing confidential data after a deal fails is firmly rooted in the Non-Disclosure Agreement (NDA), or the confidentiality sections of a broader Term Sheet or Letter of Intent.[49] These agreements serve as the primary line of legal protection and must be carefully crafted.

Defining Duties and Range

An effective NDA should unambiguously specify what is considered "Confidential Information."[50] This definition ought to be comprehensive, encompassing not only written documents but also spoken disclosures, electronic files, summaries, notes, and even the mere fact that discussions occurred.[51] Importantly, the NDA needs to include a clear "Return or Destruction" clause.[52] This clause should detail:

- Trigger Event: When the obligation takes effect (e.g., upon the termination of negotiations or upon a written request from the party sharing the information).

- Method: The recipient must decide between returning all materials or destroying them, often at the discretion of the disclosing party.

- Certification: The recipient should be required to supply a written certification (typically signed by a company officer) confirming that all materials have been returned or destroyed.[53] This establishes a distinct legal record and a point of leverage.

[48] The Bluebook: A Uniform System of Citation R. 1.1 (20th ed. 2015).
[49] JESSICA L. ARNAUD & DAVID B. ZACHARY, DEAL BREAKER: LEGAL AND PRACTICAL GUIDE TO DUE DILIGENCE IN M&A 105 (4th ed. 2024)
[50] KENNETH A. ADAMS, A MANUAL OF STYLE FOR CONTRACT DRAFTING 15.11 (4th ed. 2017) (discussing the necessity of a precise definition of confidential information)
[51] William A. Drennan, The Essential NDA: Protecting Intellectual Property in Business Negotiations, 32 Berkeley Tech. L.J. 741, 755 (2017)
[52] Robert S. Brama, The 'Return or Destruction' Clause in NDAs: Drafting for the Digital Age, 19 U. Pa. J. Bus. L. 101, 115 (2016).
[53] DOROTHY H. MEAD, TRADE SECRET LAW: A PRACTITIONER'S GUIDE § 8.2 (2025) (emphasizing the need for explicit certification to create a clear record of compliance).

Addressing Exceptions and Retention

In today's digital landscape, complete destruction of data is nearly impractical.[54] Thus, the NDA should also tackle practical exceptions. Companies frequently retain electronic versions of confidential information for regulatory or litigation reasons, known as "archival backup" or "computer-generated residual copies."[55] A strong NDA will recognize this by:

- Precisely defining what can be kept (e.g., only for compliance with regulations or as mandated by law).
- Specifying that any retained copies continue to be governed by the confidentiality and non-use obligations of the NDA indefinitely.[56] This guarantees continuous legal protection even if the physical documents have been eliminated.

Consequences for Violation

Lastly, the legal agreement must delineate the repercussions of a breach. A disclosing party would want to ensure the ability to seek injunctive relief, [57] which is a court order to immediately halt the improper use or disclosure of the information, as mere financial compensation often falls short in addressing the loss of a trade secret.[58] The NDA should also clarify which jurisdiction's laws will govern and where any disputes will be adjudicated (venue).

Strategic Considerations: Ensuring Compliance in Practice

While the contractual agreement is crucial, strategy emphasizes practical implementation, internal procedures, and proactive steps to mitigate the risk of misuse.[59]

---

[54] UNIFORM TRADE SECRETS ACT § 1(2)(ii) (NAT'L CONF. OF COMM'RS ON UNIF. STATE LAWS 1985) (recognizing trade secret protection only if reasonable efforts are made to keep the information secret).
[55]Brama, supra note 5, at 120 (discussing the challenge of "computer-generated residual copies" and litigation hold requirements)
[56] Drennan, supra note 4, at 760 (noting the importance of subjecting retained archival copies to the NDA's confidentiality obligations)
[57] W. BARRY SHURMAN & LESLIE W. GRANT, REMEDIES FOR BREACH OF CONTRACT 345 (2023) (discussing the inadequacy of monetary damages for trade secret misappropriation)
[58] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 44 cmt. d (AM. L. INST. 1995) (recognizing injunctive relief as a primary remedy for trade secret misuse)
[59] Sherer et al., Merger and Acquisition Due Diligence: A Proposed Framework, 21 Rich. J.L. & Tech. 5, 20 (2015).

Pre-Deal Preparation and Marking

Prior to any disclosure, organizations should establish internal controls. This involves:

- Clear Marking: Every confidential document should be prominently marked as "Confidential" or "Highly Confidential."[60] This demonstrates that the information has been treated as secret, enhancing the legal position in case of misuse.

- Minimizing Disclosure: Share only the information that is absolutely necessary for due diligence.[61] The less information exchanged, the lower the risk of complications after a deal breaks.

- Logging and Tracking: Keep a comprehensive log detailing what information was shared, the timing, and the individuals (including specific representatives and advisors of the other party) involved.

Execution of Return/Destruction

If the deal falls through, an immediate strategic response must be implemented:

- Formal Written Demand: Quickly send a formal request for the return or destruction of the information, citing the specific clause in the NDA.[62] This starts the compliance process and formalizes the termination of the relationship.

- Verification and Audit Rights: Companies should negotiate for, and if necessary, exercise audit rights in the NDA.[63] This enables the disclosing party to conduct a limited review to confirm that destruction has taken place, particularly for highly sensitive data. Although audit rights can be challenging to negotiate, they provide the greatest assurance.

[60] MODEL NON-DISCLOSURE AGREEMENT § 3.1 (A.B.A. Sec. Bus. Law 2020) (recommending clear labeling of materials to demonstrate reasonable security efforts)
[61] ARNAUD & ZACHARY, supra note 2, at 108 (advising on the practice of minimizing disclosure to only "need-to-know" information).
[62] Brama, supra note 5, at 122 (stressing the importance of a formal, written demand to trigger the return/destruction clock)
[63] MEAD, TRADE SECRET LAW, supra note 6, at § 8.5 (noting the strategic value of audit rights, despite the difficulty in negotiating them).

- Technical Destruction: Destroying information goes beyond merely hitting delete. Companies should insist on secure and verifiable methods, such as data wiping/sanitization for electronic files and shredding for physical documents, following industry best practices.[64]

Managing Post-Deal-Break Relationships

A strategic factor to consider is the risk that the receiving party may utilize the confidential information to compete, even indirectly. The disclosing company needs to closely monitor the business activities of the former counterparty. For information classified as a "trade secret," the obligation of confidentiality must be perpetual (i.e., it remains as long as the information is a secret).[65] A strong strategic defense includes:

- De-briefing: Conducting internal de-briefs to evaluate what information was disclosed and whether any aspect of the company's competitive advantage has been compromised.

- Relationship Management: Ending negotiations on amicable terms can sometimes lead to a smoother compliance process, as contentious relationships can complicate obtaining certifications or enforcing clauses.

lastly, effectively managing confidential information after a deal fails requires proactive legal contracting (a robust NDA with explicit return/destruction provisions) coupled with strategic execution (clear marking, accurate tracking, and swift enforcement) to protect the company's valuable secrets.

Conclusion & Suggestions

This study proves my hypothesis that **implementing legally sound Non-Disclosure Agreements (NDAs) alongside a structured, secure due diligence process significantly reduces the risk of trade secret misappropriation in mergers and acquisitions (M&A).** While NDAs are essential, standard ones often contain serious flaws such as sunset clauses that

[64] U.S. DEP'T OF DEF., NAT'L INDUS. SEC. PROGRAM OPERATING MANUAL (NISPOM) § 5-900 (recommending data wiping and sanitization for electronic media destruction).
[65] DOROTHY H. MEAD, TRADE SECRET LAW, supra note 6, at § 2.1 (explaining that a trade secret requires perpetual confidentiality protection so long as it remains a secret.

limit confidentiality duration contradicting the perpetual secrecy needed for trade secrets and ambiguous residuals clauses that make enforcement difficult. To overcome these vulnerabilities, companies must adopt a three-pronged framework. First, NDA should be carefully drafted to include explicit, enforceable return or destruction terms with signed certification necessary if negotiations fail, as well as severe limitations on residuals clauses and lifetime secrecy of trade secrets. Second, administrative and technological precautions including phased information sharing, clean teams of unbiased specialists, and Secure Virtual Data Rooms (VDRs) with granular access control and audit trails assist lower exposure risk and guarantee "reasonable measures" to preserve secrets. Lastly, immediate strategic action supported by legally binding certification and explicit written demands guarantees that private information is appropriately returned or destroyed when negotiations fall through. Businesses can successfully safeguard trade secrets and preserve their competitive edge throughout the M&A process by combining robust contracts with advanced digital controls and disciplined procedures.

Suggestions

- Establish strong Non-Disclosure Agreements (NDAs) with clear and strict regulations that protect trade secrets forever, avoid unclear "residuals" terms, and require the return or destruction of information in the event that the deal fails.

- Use secure VDR, which restricts access, keeps track of who accesses it, and allows for quick access revocation, to digitally convey critical information to prevent leaks.

- Use phased information disclosure, disclosing just what is necessary at each stage of the due diligence process, to reduce exposure risk.

- Create Clean Teams of independent experts to handle extremely sensitive competitive data on their own, especially when merging with competitors.

- Keep comprehensive logs and audit trails of who accessed sensitive data in order to hold people accountable.

- If a deal doesn't work out, insist in writing that all shared confidential information be destroyed or returned, and get a signed certification attesting to this.

- Employees and stakeholders should receive ongoing training on the value of secrecy, and contractual protections should be scrupulously adhered to long after the transaction is finished.