

**UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

SDI PRESENCE LLC,	)	
	)	
Plaintiff,	)	
	)	No. <u>1:26-cv-7289</u>
vs.	)	
	)	
GALAXIA MARTIN, and THE HACK	)	
NINJA, LLC	)	
	)	
Defendants	)	
	)	

**COMPLAINT FOR INJUNCTIVE RELIEF AND DAMAGES AND DEMAND FOR
JURY TRIAL**

Plaintiff SDI Presence LLC (“SDI” or the “Company”), by and through its undersigned counsel, and for its Complaint against Defendants Galaxia Martin (“Martin”) and The Hack Ninja, LLC (“Hack Ninja”) alleges as follows:

INTRODUCTION

1. This case arises out of Defendant Galaxia Martin's brazen breach of her contractual and other legal obligations to her now-former employer, SDI, and her theft and misuse of its intellectual property.

2. While employed by SDI and charged with developing and implementing its strategies and capabilities relating to cybersecurity, data governance, and artificial intelligence, Martin secretly formed and operated Hack Ninja as a competing business. When she identified a potentially significant market gap lying at the intersection of those three domains, she said nothing to SDI and developed a software product, THN Guardian, to capitalize on the opportunity herself.

3. In so doing, Martin and Hack Ninja (through Martin's ownership and control of the business) breached her fiduciary and contractual obligations to SDI and stole what rightfully belongs to the Company.

THE PARTIES

A. SDI Presence LLC

4. SDI is a limited liability company organized and existing under the laws of the State of Delaware, with its headquarters and principal place of business located at 200 East Randolph Street, Suite 3550, in Chicago, Illinois.

B. Galaxia Martin

5. Martin is an individual who, on information and belief, both presently and at all relevant times has lived in Shorewood, Illinois.

C. The Hack Ninja, LLC

6. Hack Ninja is a limited liability company organized and existing under the laws of the State of Illinois with its headquarters and principal place of business located at 1147 Brook Forest Avenue, Unit 649, in Shorewood, Illinois. On information and belief, Martin is the sole member and manager of Hack Ninja.

JURISDICTION AND VENUE

7. Jurisdiction is proper in this Court pursuant to 28 U.S.C. §§ 1331, 1338 because Count I of this Complaint asserts a claim under 17 U.S.C. § 201 and 28 U.S.C. § 2201 and Count II of this Complaint asserts a claim under 18 U.S.C. § 1836. This Court has jurisdiction over the remaining claims at issue in this case pursuant to 28 U.S.C. § 1367.

8. Venue is proper in this District as to all claims pursuant to 28 U.S.C. § 1391(b)(1) and (b)(2) because each defendant resides within this judicial district and a substantial part of the events giving rise to the claims at issue in this case occurred within this judicial district.

FACTUAL ALLEGATIONS

A. SDI's Business and Services

9. SDI is a national information technology ("IT") services provider and consultancy based in Chicago, Illinois, dedicated to helping public- and private-sector organizations develop and implement modernized IT systems to meet their business and security needs. SDI's managed services practice focuses on managing and supporting clients' IT infrastructure. SDI also assists clients with cloud migration and cloud infrastructure management, IT strategic planning and technology assessments, and data governance. As a trusted ServiceNow partner, SDI implements and manages the ServiceNow platform to automate and streamline client IT workflows. SDI further helps clients plan, prepare for, and leverage emerging technological innovations such as artificial intelligence ("AI"). Across all of its offerings, the Company provides its clients with a comprehensive suite of cybersecurity services to reduce clients' exposure to unauthorized access, data exfiltration, and loss.

10. SDI's data governance practice, in particular, focuses on helping clients understand what data they hold and how it moves through their systems, and advising them on the development of internal policies, standards, and processes to govern how their data is classified, accessed, managed, and protected. And as organizations increasingly adopt AI tools and platforms, these tools introduce new pathways through which sensitive data can be exposed or misused. SDI's data governance work has thus expanded to include AI readiness assessments to help clients

evaluate and update their governance frameworks and data infrastructure to meet this new challenge.

11. And of course, given today's modern enterprise IT environment, cybersecurity is foundational to everything SDI does. The Company provides clients with services to identify threats, prevent unauthorized access, and monitor their environments against security risks. A core component of that work involves protecting clients against unauthorized data loss and disclosure. This includes data lost through external attacks, compromised through insider activity, or inadvertently exposed when employees use third-party applications and platforms. SDI deploys and manages security information and event management (SIEM) systems that aggregate and analyze security event data across client networks, monitors for anomalous user behavior, and performs vulnerability scanning to identify and prioritize security weaknesses before they can be exploited. When breaches occur, SDI provides incident response services to investigate, contain, and remediate the intrusion. SDI also conducts cybersecurity and risk assessments to evaluate clients' overall security posture, advises clients on security compliance and regulatory requirements, and assists clients in implementing recognized security governance standards. SDI further provides security awareness training, including simulated social engineering attacks designed to test and strengthen clients' defenses against human-targeted cyber threats.

12. In addition to its status as a market and business leader, SDI is deeply committed to building and fostering a welcoming and supportive work environment, and to serving the communities in which it operates. As a result, SDI has been named to the Chicago Tribune's Best Places to Work list for eight consecutive years. SDI also received the National Minority Supplier Development Council's Supplier of the Year Award in 2024, a prestigious national award

recognizing SDI as a minority business enterprise that “demonstrate[s] excellence across customer service, operational growth, and community impact.”

13. SDI also donated \$1 million to City Colleges of Chicago Tech Launchpad, now a national model for driving inclusive innovation at community colleges, and co-founded Xchange Chicago, an onshore IT delivery center and apprenticeship program operating on Chicago’s South Side. Through Xchange Chicago, SDI has helped create new opportunities in South Side communities, launching both apprenticeships and full-time IT careers.

14. SDI’s commitment to its employees and its community is a core feature of the Company’s identity and mission. SDI recognizes that its business success is built upon the people and communities with which it interacts every day.

B. Martin’s Employment With SDI

15. SDI employed Martin as a Solution Director from June 2021 through May 2026. At the time she was hired, and as a condition of her employment with the Company, Martin executed a Non-Compete and Non-Solicitation Agreement, a true and correct copy of which, bearing Martin’s electronic signature, is attached hereto as Exhibit A (the “Restrictive Covenant Agreement”).

16. The Restrictive Covenant Agreement is a valid and binding contract under which Martin agreed that, during the course of her employment with SDI and for a 12-month period thereafter, she would not “engage in any business activity which is competitive with the Company nor work for any company that competes with the Company, in either case in the State of Illinois.” Ex. A at ¶ 3. The Restrictive Covenant Agreement further included customary and reasonable prohibitions on the solicitation of customers and employees, and on the use or disclosure of confidential information. *See id.* at ¶¶ 4-6.

17. In her role as a Solution Director, Martin was, in relevant part, charged with helping set the Company's strategic objectives in key areas, including cybersecurity, data governance, and AI. Reporting directly to SDI's Chief Technology Officer / Chief Operating Officer, she sat functionally between the Company's sales teams, on the one hand, and its delivery teams on the other hand. In consultation with those groups, she was responsible for identifying business opportunities and developing the solutions that SDI would take to market and worked with SDI's customers and delivery teams to ensure that those solutions were successfully implemented and deployed.

18. In the last year or so of her time with the Company, the rapid development and deployment of AI across industries, and its implications for cybersecurity and data protection, became an increasingly important area of focus both for SDI and Martin specifically. Accordingly, beginning in or around early 2025, Martin took the lead on developing and building the Company's Data and AI practice, including identifying the market opportunities that SDI could and should pursue in that space. To that end, she held monthly meetings with the Company's strategic business unit leaders, as well as the Company's delivery executives, to discuss the Company's offerings and collect feedback from customers about their needs and opportunities. She also held weekly meetings with key stakeholders involved in Data and AI-related matters or projects to ensure organizational alignment and collect feedback.

19. Indeed, the Data and AI practice was, in large measure, hers to make of what she wanted. In the modern enterprise IT environment, data governance (including data security and cybersecurity) and AI (including AI-readiness) are the most critical matters at the forefront of customers' minds and drive many of the most important enterprise IT decisions. Martin was given

the opportunity to build SDI's practice essentially from scratch to meet the needs of this burgeoning market opportunity.

20. Martin also publicly represented the Company as an expert in these areas. In late September 2025, SDI's CEO, Hardik Bhatt, put Martin in touch with Heartland Computers' ("Heartland") President, Todd Greenwald, suggesting that Martin speak as a representative of SDI at Heartland's annual OpTech conference the following month about AI-related issues. In an email dated September 29, 2025, Martin suggested that she speak on "topics related to Cybersecurity and AI."

21. The outline for her presentation, titled "AI in the Supply Chain," included a section specifically addressing "cyber considerations, such as securing data" as well as "the roadmap and governance, including data access architectures . . . privacy and compliance, AI ethics, and risk management . . ." The associated biography she submitted noted that "[a]t SDI, she develops scalable, secure, and high-performing IT solutions with the focus around Data and AI." Her final presentation materials likewise identified her as speaking for and on behalf of SDI and included an extensive discussion of "Data & AI Governance + Cybersecurity."

C. Martin's Establishment of The Hack Ninja and the Development of THN Guardian

22. Despite serving as SDI's strategic leader on cybersecurity, data governance, and AI, Martin apparently saw business opportunities in those domains that she decided to keep to herself.

23. On information and belief, in or around April 2024, Martin began operating a side business under the moniker The Hack Ninja, focused on providing cybersecurity solutions, penetration testing, and so-called "ethical hacking." Her website at the time stated that she offered "cybersecurity solutions . . . such as Data Risk Assessments" and described various additional

services including “vCISO Services,”¹ “Compliance Advis[ing],” and “Implementation and Support Services,” all of which fall well within the scope of SDI’s own offerings. Indeed, these were exactly the kinds of services that Martin was tasked with overseeing and developing at SDI.

24. Her business must have met with some success because, on February 3, 2025, Martin registered Hack Ninja as an LLC with the Illinois Secretary of State, identifying herself as its sole Manager.

25. Later in 2025, around the same time that she was pitching a presentation on issues “related to Cybersecurity and AI,” Martin began developing what would ultimately become THN Guardian: a software product that, according to The Hack Ninja’s website, “helps organizations prevent data leakage and credential compromise when using SaaS applications and AI tools such as ChatGPT, OpenAI, Azure AI, and internal AI models.”

26. According to Martin, the idea for THN Guardian arose as a result of discussions with “clients and peers about the challenges that they have with AI in regards to leaking data.” She believed that most data loss prevention systems—such as those implemented, deployed, and managed by SDI—provide no protection against the loss or exposure of sensitive data to or through common AI tools. The product was therefore designed to remedy this “dangerous blind spot[.]”

27. Though the idea falls squarely at the intersection of the cybersecurity, data governance, and AI services that Martin was supposed to develop and grow at SDI, she did not bring this opportunity to the Company. Instead, she decided that it would “pair[] really nice[ly]” with her growing Hack Ninja brand and so decided to build it in secret for herself, working on it nearly every night for months on end starting in or around November 2025.

¹ “vCISO Services” refers to virtual Chief Information Security Officer services.

28. Martin seems to have anticipated that THN Guardian had a promising commercial future. Though the product still has not publicly launched, she began advertising it on Hack Ninja's website in January 2026, around the same time that she began releasing The Hack Ninja Podcast to further evangelize the product and her business.

29. And though the product still has not been released, Martin and Hack Ninja have already widened the scope of the offering beyond the software itself to include add-ons such as managed monitoring and support, deployment and implementation assistance, and data architecture reviews, again replicating the kinds of services that SDI provides to its customers, and that Martin herself was intimately involved in.

30. As a result, from at least April 2024 until her termination in May 2026, SDI paid Martin over \$200,000 per year to help shepherd and grow its cybersecurity, data governance, and AI-related services while she worked behind the scenes to stand up a competing business providing many of the same types of services and devoted untold hours to developing the THN Guardian product to fill what she appears to have perceived as a significant and potentially lucrative gap in the exact same business sector that she was trusted with growing for SDI.

D. SDI's Discovery of Martin's Misconduct and the Termination of Martin's Employment

31. In mid-April 2026, Martin sought to capitalize on her behind-the-scenes work and approached Rusty Putzler, SDI's Chief Technology Officer and Chief Operating Officer, to ask whether the Company would be interested in entering into a partnership with Hack Ninja to license THN Guardian and deploy it to the Company's clients. She thus clearly viewed the product as one that fell comfortably within the scope of SDI's service offerings.

32. Putzler demurred and the Company immediately took steps to understand what Martin had been doing and what both Hack Ninja and THN Guardian were.

33. SDI's review revealed that Martin had been building and operating Hack Ninja as a competing business behind SDI's back and was seeking to commercialize a software product that, by all rights, belonged to SDI. The review further revealed that Martin's Hack Ninja website promotes the THN Guardian product as "patent pending."

34. Accordingly, on May 1, 2026, SDI terminated Martin's employment and demanded that she turn over all source code and assets relating to THN Guardian.

35. Martin refused and, since that time, has continued to operate Hack Ninja and to market THN Guardian in violation of SDI's rights and her legal obligations.

**COUNT I
DECLARATORY JUDGMENT
(Against Both Defendants)**

36. SDI hereby incorporates and realleges all of the preceding paragraphs of this Complaint as if they were fully set forth herein.

37. Under 17 U.S.C. § 201, ownership of any copyrightable "work made for hire" automatically rests with "the employer or other person for whom the work was prepared" and such owner or other person "is considered the author for purposes of [the Copyright Act]" unless otherwise expressly set forth in a written agreement between the parties.

38. The Copyright Act defines a "work made for hire" as including "a work prepared by an employee within the scope of his or her employment." 17 U.S.C. § 101. A copyrightable work constitutes a "work made for hire" owned by the employer if, in relevant part, it was prepared by an employee "within the scope of the employee's employment." *Baltimore Orioles, Inc. v. Major League Baseball Players Ass'n*, 805 F.2d 663, 667 (7th Cir. 1986).

39. Martin developed THN Guardian while employed by SDI to identify business opportunities relating to cybersecurity, data governance, and AI and to build out the Company's offerings in those areas. The software is a cybersecurity product intended to guard against and

mitigate risks of data loss or exposure when using AI systems. THN Guardian is, therefore, squarely within the scope of Martin's employment with SDI.

40. THN Guardian is a copyrightable work prepared by Martin during her employment with SDI and within the scope of that employment. There is no written agreement between the parties addressing the ownership of any copyrights in THN Guardian. Therefore, under 17 U.S.C. § 201, SDI is the rightful owner of all copyrights in the product, including its source code.

41. Despite this fact, Martin has asserted that she and/or Hack Ninja are the rightful owners of the product and its source code and have refused SDI's demand that she turn over the source code together with any associated assets.

42. Further, Hack Ninja continues to market THN Guardian to customers and/or potential customers.

43. Accordingly, pursuant to 28 U.S.C. § 2201, an actual controversy exists between the parties as to ownership of intellectual property rights under federal law, including copyrights and patentable inventions, in THN Guardian. SDI seeks a declaration from this Court that THN Guardian is a "work made for hire" within the meaning of 17 U.S.C. § 201, and that SDI is the rightful owner of all copyrights in the product, including in its source code and any associated assets, as well as such other relief as the Court may deem just and proper.

COUNT II
VIOLATION OF THE DEFEND TRADE SECRETS ACT
(Against Both Defendants)

44. SDI hereby incorporates and realleges all of the preceding paragraphs of this Complaint as if they were fully set forth herein.

45. As set forth above, the source code to THN Guardian, together with its associated assets, belong to SDI.

46. SDI takes reasonable steps to protect documents and information such as the source code to THN Guardian. These steps include, but are not necessarily limited to:

- a. requiring employees to execute agreements such as the Restrictive Covenant Agreement which prohibits employees from using or disclosing the Company's secret or confidential information, including trade secrets, other than in connection with their work for the Company, and requiring employees to promptly return all such information to the Company following the termination of their employment, without retaining any copies for themselves; and
- b. promulgating and enforcing an Information Security Policy that, in relevant part, restricts employees' access to confidential information and limits the manner and circumstances in which confidential information can be used and disclosed.

47. The THN Guardian source code derives, or is expected to derive, independent economic value by virtue of the fact that it is not generally known to others and cannot be readily ascertainable by proper means by any other person or entity who might be willing or able to commercialize the product.

48. The THN Guardian source code is, therefore, a "trade secret" within the meaning of 18 U.S.C. § 1839.

49. THN Guardian is intended for use in interstate or foreign commerce within the meaning of 18 U.S.C. § 1836. Martin and Hack Ninja are already marketing the product online and the product is marketed for use by any person, business, or entity who is concerned with the disclosure or loss of data through or to AI tools, regardless of where those persons or entities may be located.

50. Martin and Hack Ninja have refused to turn over the THN Guardian source code and its associated assets and are continuing to actively market the product to potential customers without SDI's approval or consent and despite having been previously informed of SDI's ownership. Further, because Martin developed the product as a "work for hire," she and Hack Ninja each acquired the source code under circumstances giving rise to a duty to maintain the secrecy of that code and to limit their use of the code for SDI's own business purposes and, in the case of Hack Ninja, derived from or through a person who owed a duty to SDI to maintain the secrecy of the code and limit its use for SDI's business purposes. Further, they were each aware of Martin's duties because, among other things, they were set forth in the Restrictive Covenant Agreement that Martin signed, and in the Information Security Policy that she electronically acknowledged on multiple occasions during the course of her employment.

51. Therefore, Martin and Hack Ninja have each misappropriated the THN Guardian source code within the meaning of 18 U.S.C. § 1839.

52. Martin and Hack Ninja's conduct has proximately caused damages to SDI by depriving the Company of the possession and use of its confidential and trade secret information, by risking the further disclosure of such information to other third-parties, and by depriving SDI of the opportunity to commercialize the product for its own business purposes and derive revenues therefrom, and to establish itself as an early leader in the market space that Martin identified as a ripe opportunity.

53. Accordingly, pursuant to 18 U.S.C. § 1836, SDI asks this Court to enter an order:

- a. Requiring Martin and Hack Ninja to turn over to SDI a complete copy of the THN Guardian source code, together with any other associated assets, and to then delete

and/or destroy any copies of any such information in their possession, custody, or control;

- b. Permanently enjoining Martin and Hack Ninja from marketing, selling, licensing, disseminating, or otherwise using or disclosing the THN Guardian product or any of its source code or other associated assets;
- c. Requiring Martin and Hack Ninja each to disgorge any profits made on the sale, licensing, or dissemination of THN Guardian or its source code or other associated assets;
- d. Requiring Martin and Hack Ninja each to pay to SDI an amount to be determined at trial to compensate SDI for the damages caused by Defendants' misappropriation; and
- e. Providing for such other relief as the Court may deem just and proper.

**COUNT III
VIOLATION OF THE ILLINOIS TRADE SECRETS ACT
(Against Both Defendants)**

54. SDI hereby incorporates and realleges all of the preceding paragraphs of this Complaint as if they were fully set forth herein.

55. As set forth above, the source code to THN Guardian, together with its associated assets, belong to SDI.

56. SDI takes reasonable steps to protect documents and information such as the source code to THN Guardian. These steps include, but are not necessarily limited to:

- a. requiring employees to execute agreements such as the Restrictive Covenant Agreement which prohibits employees from using or disclosing the Company's secret or confidential information, including trade secrets, other than in connection with their work for the Company, and requiring employees to promptly return all

such information to the Company following the termination of their employment, without retaining any copies for themselves; and

- b. promulgating and enforcing an Information Security Policy that, in relevant part, restricts employees' access to confidential information and limits the manner and circumstances in which confidential information can be used and disclosed.

57. The THN Guardian source code derives, or is expected to derive, independent economic value by virtue of the fact that it is not generally known to others and cannot be readily ascertainable by proper means by any other person or entity who might be willing or able to commercialize the product.

58. The THN Guardian source code is, therefore, a "trade secret" within the meaning of 765 ILCS 1065/2.

59. Martin and Hack Ninja have refused to turn over the THN Guardian source code and its associated assets and are continuing to actively market the product to potential customers without SDI's approval or consent and despite having been previously informed of SDI's ownership. Further, because Martin developed the product as a "work for hire," she and Hack Ninja each acquired the source code under circumstances giving rise to a duty to maintain the secrecy of that code and to limit their use of the code for SDI's own business purposes and, in the case of Hack Ninja, derived from or through a person who owed a duty to SDI to maintain the secrecy of the code and limit its use for SDI's business purposes. Further, they were each aware of Martin's duties because, among other things, they were set forth in the Restrictive Covenant Agreement that Martin signed, and in the Information Security Policy that she electronically acknowledged on multiple occasions during the course of her employment.

60. Therefore, Martin and Hack Ninja have each misappropriated the THN Guardian source code within the meaning of 765 ILCS 1065/2.

61. Martin and Hack Ninja's conduct has proximately caused damages to SDI by depriving the Company of the possession and use of its confidential and trade secret information, by risking the further disclosure of such information to other third-parties, and by depriving SDI of the opportunity to commercialize the product for its own business purposes and derive profits therefrom, and to establish itself as an early leader in the market space that Martin identified as a ripe opportunity.

62. Accordingly, pursuant to 765 ILCS 1065/3 and 1065/4, SDI asks this Court to enter an order:

- a. Requiring Martin and Hack Ninja to turn over to SDI a complete copy of the THN Guardian source code, together with any other associated assets, and to then delete and/or destroy any copies of any such information in their possession, custody, or control;
- b. Permanently enjoining Martin and Hack Ninja from marketing, selling, licensing, disseminating, or otherwise using or disclosing the THN Guardian product or any of its source code or other associated assets;
- c. Requiring Martin and Hack Ninja each to disgorge any profits made on the sale, licensing, or dissemination of THN Guardian or its source code or other associated assets;
- d. Requiring Martin and Hack Ninja each to pay to SDI an amount to be determined at trial to compensate SDI for any damages caused by Defendants' misappropriation; and

- e. Providing for such other relief as the Court may deem just and proper.

COUNT IV
BREACH OF FIDUCIARY DUTIES
(Against Defendant Martin)

63. SDI hereby incorporates and realleges all of the preceding paragraphs of this Complaint as if they were fully set forth herein.

64. During her employment with SDI, Martin was entrusted with identifying business opportunities, setting the Company's business objectives and go-to-market strategies, and building the solutions to meet customers' needs.

65. Under Illinois law, all employees owe their employer a fiduciary duty of loyalty. Higher-level employees such as Martin owe heightened duties by virtue of their roles and responsibilities and the trust placed in them by their employers.

66. Martin's decision to establish Hack Ninja and to use it as a vehicle to engage in blatant competition with SDI while still employed constitutes a flagrant violation of her fiduciary duties to the Company.

67. Martin further breached her fiduciary duties to SDI by failing to present the idea of developing, marketing, and/or partnering with a vendor to provide, a product to SDI's customers to address the "dangerous blind spot[]" she had identified in most data loss prevention services.

68. Instead, in further violation of her duties and responsibilities, she kept that idea to herself and sought to exploit it for her own personal profit by developing the THN Guardian product and using Hack Ninja as the vehicle to commercialize it.

69. From at least April 2024 onward, Martin secretly deprived SDI of the benefit of a loyal and faithful employee, competed with the Company behind its back, kept business opportunities to herself to exploit for her own gain, and has sought to commercialize a product that rightfully belongs to the Company, all in violation of her fiduciary duties to the Company.

70. Martin's conduct has proximately caused damages to SDI by depriving it of the loyalty to which it was entitled from her and for which she was handsomely paid, and by depriving it of the opportunity to pursue the business opportunities that Martin kept for herself and to derive any profits therefrom, and to establish itself as an early leader in the market space that Martin identified as a ripe opportunity.

71. Accordingly, SDI asks this Court to enter an order:

- a. Requiring Martin to repay to the Company the full amount of any salary, other compensation, and other benefits paid and/or provided to her since April 2024 or, if earlier, since she commenced operating Hack Ninja as a competing business;
- b. Requiring Martin to disgorge any income and/or profits she has earned or received while employed by SDI, whether directly or indirectly, from her operation of Hack Ninja and/or from the sale, licensing, or dissemination of THN Guardian or its source code or other associated assets;
- c. Requiring Martin and Hack Ninja each to pay to SDI an amount to be determined at trial to compensate SDI for any damages caused by Martin's breaches;
- d. Requiring Martin and Hack Ninja to pay punitive damages; and
- e. Providing for such other relief as the Court may deem just and proper.

COUNT V
BREACH OF CONTRACT
(Against Defendant Martin)

72. SDI hereby incorporates and realleges all of the preceding paragraphs of this Complaint as if they were fully set forth herein.

73. In connection with and as a condition of her employment with SDI, Martin signed the Restrictive Covenant Agreement, which is a valid and binding contract under Illinois law.

74. The Restrictive Covenant Agreement, in relevant part, states as follows:

- a. “Employee agrees that during the term of Employee’s employment with the Company and for a period of twelve (12) months from the date of termination of Employee’s employment with the Company for any reason (the “Restricted Period”), Employee will not engage in any business activity which is competitive with the Company nor work for any company that competes with the Company, in either case in the State of Illinois.” (the “Non-Competition Covenant”).
- b. “During the Restricted Period and for all periods thereafter, Employee agrees not to disclose or make use of, for Employee’s benefit or for the benefit of a business or entity other than the Company, any secret or confidential information, business opportunities, contacts, customer lists and lists of prospective customers, the names or addresses of any of the customers or clients of the Company or any other information pertaining to them, or any other information of or pertaining to the Company, its suppliers, business, products, technology, analysis, research, processes, ‘know how,’ services, pricing [or] financial affairs (collectively, the ‘Confidential Information.’) Employee agrees that access to and permission to use Company’s computer systems and equipment, Confidential Information and all Company information contained therein is restricted to legitimate business purposes on behalf of the Company during the term of Employee’s employment with the Company. Employee agrees that upon termination of employment with the Company, regardless of the cause therefore, or at Company’s request, Employee will promptly return, transfer to the Company, or destroy all property and Confidential Information provided by the Company...” (the “Confidentiality Covenant”).

75. SDI has performed all of its obligations under the Restrictive Covenant Agreement.

76. Martin's establishment and operation of Hack Ninja while employed by SDI, and her continued operation of Hack Ninja after her termination, constitutes a flagrant violation of the Non-Competition Covenant.

77. Further, Martin's use of the THN Guardian source code and its associated assets, all of which properly belong to SDI, constitutes a flagrant violation of the Confidentiality Covenant.

78. Martin's conduct has proximately caused damages to SDI by depriving it of the full benefits of her compliance with her contractual obligations both during and subsequent to her employment, suffering the loss and misuse of its confidential trade secret information that is now being put to commercial use by Martin herself who is seeking to use that information to compete with SDI and deny it the benefit of those profits that it otherwise could have obtained, and by the loss of the opportunity to establish itself as an early leader in the market space that Martin identified as a ripe opportunity.

79. Accordingly, SDI asks this Court to enter an order:

- a. Enjoining Martin's continued operation of Hack Ninja until the end of the Restricted Period;
- b. Enjoining Martin from continuing to use and/or disclose the THN Guardian product, source code, or any other associated assets;
- c. Requiring Martin and Hack Ninja each to pay to SDI an amount to be determined at trial to compensate SDI for any damages caused by Martin's breaches; and
- d. Providing for such other relief as the Court may deem just and proper.

COUNT VI
AIDING AND ABETTING BREACH OF FIDUCIARY DUTIES
(Against Defendant Hack Ninja)

80. SDI hereby incorporates and realleges all of the preceding paragraphs of this Complaint as if they were fully set forth herein.

81. Hack Ninja aided and abetted Martin's breach of her fiduciary duties to SDI by serving as the vehicle through which she competed with the Company, and by marketing and seeking to sell and/or license the THN Guardian software, in each case while fully aware that Martin was still employed by SDI.

82. In so-doing, Hack Ninja acted together with Martin and provided substantial support and assistance to her to facilitate the breach of her fiduciary duties to the Company.

83. Hack Ninja's conduct has proximately caused damages to SDI by depriving it of the loyalty to which it was entitled from Martin and for which she was handsomely paid, and by depriving it of the opportunity to pursue the business opportunities that Martin kept for herself and to derive any profits therefrom, and to establish itself as an early leader in the market space that Martin identified as a ripe opportunity.

84. Accordingly, SDI asks this Court to enter an order:

- a. Enjoining Hack Ninja's continued competition with SDI until the end of the Restricted Period;
- b. Enjoining Hack Ninja's continued marketing, licensing, sale, and/or distribution of THN Guardian;
- c. Requiring Hack Ninja to pay to SDI an amount to be determined at trial to compensate SDI for any damages caused by Martin's breaches;
- d. Requiring Martin and Hack Ninja to pay punitive damages; and
- e. Providing for such other relief as the Court may deem just and proper.

COUNT VII
TORTIOUS INTERFERENCE WITH CONTRACT
(Against Defendant Hack Ninja)

85. SDI hereby incorporates and realleges all of the preceding paragraphs of this Complaint as if they were fully set forth herein.

86. Hack Ninja knew that Martin had entered into and was bound by the Restrictive Covenant Agreement.

87. Nevertheless, Hack Ninja has actively marketed and sought to sell and/or license the THN Guardian software that Martin provided to Hack Ninja in violation of the Confidentiality Covenant. Further, on information and belief, both while Martin was employed by SDI and thereafter, Hack Ninja has entered into, and has continued to enter into, contracts with customers for the performance of services for customers that are competitive with those services provided by SDI, despite knowing full-well that such activities constitute a direct violation of the Non-Competition Covenant.

88. Hack Ninja has thus intentionally and unjustifiably sought to induce and/or cause Martin to breach, and continue to breach, her contractual obligations to SDI.

89. Hack Ninja's conduct has proximately caused damages to SDI by depriving it of the full benefits of her compliance with her contractual obligations both during and subsequent to her employment, suffering the loss and misuse of its confidential trade secret information that is now being put to commercial use by Martin and Hack Ninja who are seeking to use that information to compete with SDI and deny SDI the benefit of those profits that it otherwise could have obtained, and by the loss of the opportunity to establish itself as an early leader in the market space that Martin identified as a ripe opportunity.

PRAYER FOR RELIEF

90. WHEREFORE, by virtue of the foregoing allegations, SDI asks this Court to issue an order:

- a. Declaring and confirming that SDI is the sole owner of all right, title, and interest in THN Guardian, its source code, and any associated assets;
- b. Requiring Martin and Hack Ninja to turn over to SDI a complete copy of the THN Guardian source code, together with any other associated assets, and to then delete and/or destroy any copies of any such information in their possession, custody, or control;
- c. Enjoining Hack Ninja's continued competition with SDI until the end of the Restricted Period;
- d. Permanently enjoining Martin and Hack Ninja from marketing, selling, licensing, disseminating, or otherwise using or disclosing the THN Guardian product or any of its source code or other associated assets;
- e. Requiring Martin and Hack Ninja each to disgorge any profits made on the sale, licensing, or dissemination of THN Guardian or its source code or other associated assets;
- f. Requiring Martin to repay to the Company the full amount of any salary, other compensation, and other benefits paid and/or provided to her since April 2024 or, if earlier, since she commenced operating Hack Ninja as a competing business;
- g. Requiring Martin to disgorge any income and/or profits she has earned or received while employed by SDI, whether directly or indirectly, from her operation of Hack

Ninja and/or from the sale, licensing, or dissemination of THN Guardian or its source code or other associated assets;

- h. Requiring Martin and Hack Ninja each to pay to SDI an amount to be determined at trial to compensate SDI for the damages caused by Defendants' misconduct;
- i. Requiring Martin and Hack Ninja to pay punitive damages;
- j. Requiring Martin and Hack Ninja each to pay SDI's costs and attorneys' fees incurred in connection with this litigation; and
- k. Providing such other relief as the Court may deem just and proper.

JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38, SDI hereby demands a trial by jury on all issues so triable.

Date: June 22, 2026

Respectfully submitted,

By: /s/ Corwin J. Carr

Corwin J. Carr
Thomas M. Williams
M. Olivia Glass
BARACK FERRAZZANO KIRSCHBAUM
& NAGELBERG, LLP
200 West Madison Street, Suite 3900
Chicago, IL 60606
Tel: 312-984-3100
Fax: 312-984-3150
corwin.carr@bfkn.com
tom.williams@bfkn.com
olivia.glass@bfkn.com
Counsel for Plaintiff