

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

MAGNET FORENSICS, LLC,

Plaintiff,

v.

MARIO DEL GAUDIO and PARADIGM
SHIFT TECHNOLOGY, S.L.,

Defendants.

Civil Action No.

**MEMORANDUM OF LAW IN SUPPORT OF
PLAINTIFF’S EMERGENCY MOTION FOR TEMPORARY
RESTRAINING ORDER AND PRELIMINARY INJUNCTION**

Plaintiff Magnet Forensics, LLC (“Magnet Forensics”) respectfully submits this Memorandum of Law in support of its Emergency Motion for Temporary Restraining Order and Preliminary Injunction against Defendants Mario Del Gaudio (“Del Gaudio”) and Paradigm Shift Technology, S.L., (“Paradigm Shift”) (collectively, “Defendants”).

I. INTRODUCTION

This case involves the brazen misappropriation and public disclosure of one of Magnet Forensics’ most valuable trade secrets: a proprietary A12/A13 SecureROM access capability developed through years of research investment and substantial resources. Del Gaudio, a former engineer who had direct access to this

capability during his placement with Magnet Forensics, collaborated with his new employer, Paradigm Shift, to publish the access capability in a publicly accessible blog post on June 18, 2026. The blog post remains live. It has been reshared across the technology and cybersecurity community by outlets including TechCrunch, Mashable, SecurityWeek, The Hacker News, Infosecurity Magazine, Security Affairs, and TechRadar. And every day it remains publicly accessible, the trade secret's value erodes irreversibly.

Courts in this District routinely grant emergency injunctive relief in trade secret cases far less egregious than this one. *See, e.g., Priority Payment Sys., LLC v. Signapay, LTD*, 161 F. Supp. 3d 1294, 1306 (N.D. Ga. 2016) (Totenberg, J.) (granting preliminary injunction where contractor misappropriated source code and transferred it to competitor); *Arclin USA, LLC v. Vits Tech. GmbH*, No. 1:20-cv-01197, 2020 WL 10056276, at *10 (N.D. Ga. Apr. 29, 2020) (Brown, J.) (granting preliminary injunction where manufacturer used confidential information to build competing product); *SGS N. Am. Inc. v. Hartquist*, No. 1:25-cv-00586-ELR, 2025 WL 1779388, at *8 (N.D. Ga. Mar. 6, 2025) (Ross, J.) (granting preliminary injunction based on acquisition of trade secrets alone, without evidence of disclosure to third parties); *Sungdo Eng USA, Inc. v. Hyoungwon Inc.*, No. 1:23-cv-6025-MLB, 2024 WL 671582, at *2 (N.D. Ga. Jan. 26, 2024) (Brown, J.) (granting TRO where former employee stole confidential bid and submitted it on behalf of competitor);

Solvay Specialty Polymers USA, LLC v. Liu, No. 1:18-cv-02120, Dkt. 6 (Order) (N.D. Ga. May 14, 2018) (Ross, J.) (granting ex parte TRO where employee systematically downloaded trade secrets). In each of those cases, the court found injunctive relief warranted based on circumstantial evidence and the threat of future harm. Here, Magnet Forensics presents direct evidence of misappropriation, and the harm is not merely threatened—it is ongoing and accelerating. If those cases warranted emergency relief, this one compels it.

Emergency relief is warranted because Magnet Forensics satisfies each of the four factors required for injunctive relief. Magnet Forensics is substantially likely to succeed on the merits of its claims under the Defend Trade Secrets Act (“DTSA”), the Georgia Trade Secrets Act (“GTSA”), and for breach of contract. The harm is irreparable because once a trade secret is publicly disclosed, its confidentiality cannot be restored. The balance of equities overwhelmingly favors Magnet Forensics because Defendants have no right to possess or publish Magnet Forensics’ proprietary information. And the public interest supports the enforcement of trade secret protections and contractual obligations.

II. STATEMENT OF FACTS

Magnet Forensics incorporates by reference the factual allegations set forth in its Verified Complaint. The material facts are undisputed for purposes of this Motion and are summarized as follows:

A. Magnet Forensics and Its Business

Magnet Forensics is a leading provider of specialized digital investigation solutions used by more than 6,000 public and private sector entities in over 100 countries, including law enforcement agencies, intelligence agencies, and government entities. (Compl. ¶¶ 15-18.) Its customers rely on Magnet Forensics' tools to conduct sensitive investigative operations. (*Id.* ¶ 18.)

Among Magnet Forensics' most valuable proprietary capabilities is a class of tools known as "access capabilities," which are specialized methodologies developed to gain access to digital devices. (*Id.* ¶¶ 19-20.) The development of these exploits requires deep technical expertise, years of research investment, and significant proprietary investment. (*Id.* ¶ 22.)

B. Magnet Forensics' Protection of Its Trade Secrets

Magnet Forensics takes extensive and reasonable steps to protect the secrecy of its confidential and trade secret information. (*Id.* ¶ 23.) These measures include: (i) technology-based protections, including password-protected and encrypted computer systems and electronic databases; (ii) restricting disclosure of confidential and trade secret information to individuals who have a legitimate business need to access such information on a need-to-know basis; (iii) requiring individuals who have access to confidential and trade secret information, including employees and those who otherwise perform services on its behalf, to execute restrictive covenant

agreements containing non-disclosure, intellectual property assignment, and return-of-property provisions; and (iv) employing physical security measures and access controls at its facilities and limiting access to its most sensitive research and development projects, including access capability development, to a small number of authorized personnel. (*Id.* ¶¶ 24-26.)

C. The A12/A13 SecureRom Access Capability

The A12/A13 SecureROM access capability at issue (internally designated “MSG”) was developed through years of research, deep technical expertise, and significant proprietary investment. (*Id.* ¶¶ 33, 61.) The MSG capability is integral to the functionality of Magnet Forensics’ forensics products, which are used by law enforcement agencies and government agencies to conduct investigations. (*Id.* ¶¶ 16-18, 62.) The confidentiality of the MSG capability is essential not only to Magnet Forensics’ competitive position but also to the integrity of sensitive investigative operations that depend on the capability remaining non-public. (*Id.* ¶ 64.)

D. Del Gaudio’s Placement and Contractual Obligations

Del Gaudio served as an Exploit Engineer at Magnet Forensics from November 2023 through November 2024, during which time he had direct access to and participated in the development of the A12/A13 SecureROM access capability. (*Id.* ¶¶ 30, 32.) Specifically, Del Gaudio participated in weekly team meetings at which the details of Magnet Forensics’ MSG capability, as well as Magnet

Forensics' access strategy were discussed in depth. (*Id.* ¶ 33.) These meetings addressed, among other things, the specialized tools needed to perform the research that led to the discovery of the MSG capability, the custom hardware required to communicate with the target device in order to trigger the vulnerability, and the access strategy needed to gain control of the device's system. (*Id.*) Del Gaudio's regular participation in these meetings gave him repeated, direct exposure to the full scope of the MSG capability and Magnet Forensics' proprietary approach to exploiting the underlying vulnerability. (*Id.*)

As early as April 2024, Magnet Forensics engineers discussed the technical details of the A12/A13 SecureROM vulnerability in meetings in which Del Gaudio participated. (*Id.* ¶ 34.) In May 2024, the MSG capability was integrated into one of Magnet Forensics' products, a milestone that was discussed in the weekly standups Del Gaudio attended. (*Id.*) Del Gaudio was therefore aware not only of the MSG capability's technical architecture but also of its integration into Magnet Forensics' commercial product line and its operational significance to Magnet Forensics' business. (*Id.*) In addition, Del Gaudio was specifically tasked with designing a separate, unrelated tool for testing another capability. (*Id.* ¶ 35.) In order to test that tool, however, Del Gaudio was required to make use of the MSG capability. Del Gaudio executed the MSG capability likely dozens of times in the course of this

work, giving him hands-on, intimate familiarity with the access and capabilities that the MSG capability provided. (*Id.*)

As condition of his placement, Del Gaudio executed a Proprietary Rights, Intellectual Property, and Restrictive Covenants Agreement (the “Agreement”) imposing comprehensive surviving obligations. (*Id.* ¶¶ 37-57.) Under the Agreement, Del Gaudio:

- (1) acknowledged his placement was one of “trust and responsibility with access to Confidential Information, trade secrets, and other information concerning employees and customers of the Company.” Agreement § 1.2.
- (2) agreed not to “directly or indirectly: (i) misappropriate, disclose, transfer, assign, disseminate or otherwise communicate or make available...to any person or entity any Confidential Information.” Agreement § 5.1.
- (3) agreed that “during his placement with the Company and any time afterwards all Materials shall be the sole and exclusive property of the Company” and agreed to “hold all Materials in trust and strict confidence for the Company and its clients, without disclosing such information to any third parties, whether contained in Employee’s memory or embodied in writing or other physical form.” Agreement § 3.2.
- (4) irrevocably assigned to Magnet Forensics “all worldwide patents, patent applications, copyrights, mask works, trade secrets and other intellectual

property rights in any Company Invention” and waived all “Moral Rights,” including “any right . . . to control the publication or distribution of any Company Invention.” Agreement § 4.4.

(5) acknowledged that “a breach of any section of this Agreement will cause serious harm to the Company” and agreed that “the Company shall be entitled to specific performance and any injunctive or other equitable relief as a remedy for any such breach.” Agreement §§ 10.2, 10.3.

E. The Publication and Defendants’ Refusal to Comply

On June 18, 2026, Paradigm Shift, an entity operating in the technology and cybersecurity industry seeking to monetize access capabilities, published a detailed technical blog post titled “Introducing usbliter8: An A12/A13 SecureROM Exploit” (the “Publication”), which disclosed extensive technical details regarding a proprietary exploit that makes use of the same proprietary vulnerability discovered by Magnet Forensics and developed into an access capability to which Del Gaudio had access during his placement with Magnet Forensics . (Compl. ¶¶ 66, 68-69.)¹

¹ As noted in the Complaint, Magnet Forensics did not attach the Blog Post as an exhibit to the Complaint, nor did it provide a link to the Blog Post, since doing so would further publicly disseminate the very trade secret information that Magnet Forensics seeks to protect in this action. Magnet Forensics will promptly make the full text of the Blog Post available to the Court for in camera review upon request, or under such protective conditions as the Court deems appropriate, to avoid compounding the harm caused by Defendants’ unauthorized disclosure.

The correlation between the technical details in the Publication and Magnet Forensics' proprietary capability is not coincidental. (*Id.* ¶ 69.) Magnet Forensics has identified direct and compelling evidence linking Del Gaudio to the Publication. (*Id.* ¶ 70.) A preserved screenshot connects Del Gaudio's name and photograph to the @NotHdesk account associated with the Publication, and the @NotHdesk account identifier is directly connected to Del Gaudio's known personal email address, mario@athdesk.me. (*Id.*) Additionally, Paradigm Shift itself acknowledged that it coordinated disclosure with Apple Product Security prior to publication, confirming that it understood the sensitivity and provenance of the information it possessed. (*Id.* ¶ 74.)

Despite receiving cease-and-desist letters from Magnet Forensics' counsel on June 18 and June 19, 2026, as well as a final demand on June 26, 2026, Defendants have refused to remove the Publication or take any remedial action. (*Id.* ¶¶ 76-85.)

F. The Cascading and Accelerating Harm

The Publication has been rapidly amplified across the technology and cybersecurity media landscape. Within days of the initial blog post, the story was picked up by TechCrunch, Mashable, SecurityWeek, The Hacker News, Infosecurity Magazine, Security Affairs, TechRadar, Gadget Hacks, TechRepublic, and Cyber Insider, among others. (*Id.* ¶ 85.) A Reddit thread about the access capability appeared the same day as the Publication. (*Id.*) Each additional republication and

reshare extends the reach of the misappropriated trade secret to new audiences—including Magnet Forensics’ direct competitors, independent security researchers, and the device manufacturer, Apple. (*Id.*)

The harm from this disclosure is cascading and accelerating in three critical dimensions. First, the public disclosure of the MSG capability has alerted Apple to the vulnerability, which will cause Apple to seek to mitigate it. (*Id.* ¶ 60.) If Apple patches the vulnerability, the MSG capability will become permanently valueless, directly impacting the data access capabilities of Magnet Forensics’ forensic products. (*Id.*) Second, the disclosure allows competitors to potentially utilize the MSG capability to release competitive products supporting the affected devices, eroding the competitive advantage that Magnet Forensics developed through years of investment. (*Id.* ¶ 109.) Third, the public disclosure of the MSG capability’s existence and methodology undermines the trust and confidence of Magnet Forensics’ law enforcement and government customers, who depend on the absolute confidentiality of these capabilities. (*Id.*)

Every day that the Publication remains accessible, these harms compound. The Court can stop the bleeding, even if it cannot undo the wound.

III. LEGAL STANDARD

A temporary restraining order is appropriate when the movant demonstrates: (1) a substantial likelihood of success on the merits; (2) a substantial threat of

irreparable injury absent injunctive relief; (3) the threatened injury to the movant outweighs the harm the injunction may cause the opposing party; and (4) granting the injunction will not disserve the public interest. *Siegel v. LePore*, 234 F.3d 1163, 1176 (11th Cir. 2000). “To support a preliminary injunction, a district court need not find that the evidence positively guarantees a final verdict in plaintiff’s favor.” *Levi Strauss & Co. v. Sunrise Int’l Trading Inc.*, 51 F.3d 982, 985 (11th Cir. 1995).

The DTSA expressly authorizes injunctive relief “to prevent any actual or threatened misappropriation” of trade secrets, “provided the order does not...prevent a person from entering into an employment relationship.” 18 U.S.C. § 1836(b)(3)(A). The GTSA similarly authorizes injunctive relief to enjoin “[a]ctual or threatened misappropriation.” O.C.G.A. § 10-1-762(a). Injunctive relief is “especially proper and routinely granted” in trade secret cases. *See Solvay*, No. 1:18-cv-02120, Dkt. 6 (N.D. Ga. May 14, 2018) (Ross, J.) (granting ex parte TRO); *see Priority Payment Sys.*, 161 F. Supp. 3d at 1304 (granting preliminary injunction).

IV. ARGUMENT

A. Magnet Forensics Is Substantially Likely to Succeed on the Merits

Magnet Forensics is substantially likely to prevail on each of its claims. The strength of each is addressed in turn.

1. *Federal Trade Secret Misappropriation (DTSA)*

To establish a claim under the DTSA, a plaintiff must show: (1) it possessed a trade secret; (2) the defendant misappropriated the trade secret; and (3) the trade secret was related to a product or service used in, or intended for use in, interstate or foreign commerce. 18 U.S.C. § 1836(b)(1).²

a. The A12/A13 SecureROM Exploit Is a Protectable Trade Secret

A “trade secret” under the DTSA is “all forms and types of financial, business, scientific, technical, economic, or engineering information” that “(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.” 18 U.S.C. § 1839(3).

The A12/A13 SecureROM access capability and its underlying methodology satisfy both prongs. Magnet Forensics took extensive measures to protect the access capability’s secrecy, including: (i) limiting access on a need-to-know basis; (ii) maintaining information in password-protected and encrypted electronic databases;

² The trade secret at issue relates to services used in interstate and foreign commerce. Magnet Forensics serves customers across the United States and in more than 100 countries. (Compl. ¶ 18.) Thus, this DTSA element is satisfied. *See Solvay Specialty Polymers USA, LLC v. Zhenguo (Leo) Liu*, 331 F.R.D. 187, 191 (N.D. Ga. 2019) (commerce element satisfied at injunction stage where plaintiff alleged its products were used in interstate and foreign commerce).

(iii) restricting access to access capability-development projects to a small number of authorized personnel; (iv) employing physical security measures and access controls at its facilities; and (v) requiring individuals with access to execute restrictive covenant agreements containing non-disclosure, intellectual property assignment, and return-of-property provisions. (Compl. ¶¶ 23-26.)

These protections meet or exceed the measures that courts in this District have found sufficient to satisfy the reasonable-measures requirement. *See Priority Payment Sys.*, 161 F. Supp. 3d at 1300 (finding reasonable measures where employer used confidentiality provisions in contracts, Employee/Contractor Security Policy, Data Security Policy, access limitations based on job responsibilities, prevention of file sharing to outside parties, annual security training and certification, and sophisticated external firewall protections); *SGS*, 2025 WL 1779388, at *1-2 (finding reasonable measures where employer maintained Code of Integrity, Confidentiality Agreement, and employee Handbook with confidentiality provisions); *Arclin*, 2020 WL 10056276, at *1 (finding reasonable measures through a series of confidentiality agreements executed throughout the parties' relationship).

The access capability also derives independent economic value from its confidentiality. It enables Magnet Forensics' more than 6,000 customers in over 100 countries to access, recover, and preserve digital evidence from devices that would otherwise remain inaccessible. (Compl. ¶ 62.) The access capability is the product

of years of research, deep technical expertise, and significant investment that is not readily ascertainable by proper means. As the court recognized in *Priority Payment Systems*, proprietary capabilities developed “at great expense over several years” with “unique capabilities” and “competitive functional[ity]” possess the economic value required for trade secret protection. 161 F. Supp. 3d at 1299. Moreover, the fact that a capability may address a known type of vulnerability does not diminish its trade secret status. As the Georgia Supreme Court has held, “a trade secret process may be established even if known components are assembled and known techniques are combined to produce a useful process which is not known in the industry.” *Essex Group, Inc. v. Southwire Co.*, 269 Ga. 553, 555 (1998); *see also Priority Payment Sys.*, 161 F. Supp. 3d at 1300 n.3 (rejecting argument that use of public specifications precluded trade secret protection, citing *Essex Group*). What makes the A12/A13 SecureROM access capability a trade secret is not the existence of the vulnerability itself, but the proprietary methodology, architecture, implementation details, and operational deployment information that Magnet Forensics developed through years of extensive research and significant investment to exploit it—information that was not generally known and not readily ascertainable before Defendants’ unauthorized disclosure. (Compl. ¶¶ 61, 64-65, 69.)

b. Defendants Misappropriated the Trade Secret

“Misappropriation” under the DTSA includes the “disclosure or use of a trade secret of another without express or implied consent by a person who . . . at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was...acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret.” 18 U.S.C. § 1839(5)(B)(ii)(II). Misappropriation also includes the “acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means.” *Id.* § 1839(5)(A).

Del Gaudio’s Misappropriation. Del Gaudio acquired knowledge of the A12/A13 SecureROM access capability during his placement with Magnet Forensics, under circumstances giving rise to a clear duty of confidentiality under the Agreement. (Compl. ¶¶ 32-36.) He disclosed this information to Paradigm Shift, and together they published it to the world. Neither had Magnet Forensics’ authorization. (*Id.* ¶ 72.)

The evidence against Del Gaudio is more compelling than mere circumstantial inference. In *SGS*, Judge Ross found misappropriation established where the evidence showed acquisition of trade secrets through downloading onto personal devices via USB drives and email—even where the defendant swore he had never disclosed the information to any third party. 2025 WL 1779388, at *6. The court held that acquisition alone, in breach of a duty to maintain secrecy, constitutes

misappropriation under both the DTSA and the GTSA. *Id.* If acquisition without disclosure warrants injunctive relief, then acquisition followed by global publication compels it.

Here, the evidence goes well beyond acquisition. The preserved screenshot linking Del Gaudio’s name and photograph to the @NotHdesk account associated with the Publication, the confirmed connection between that account and his personal email address, and his documented assignment to the precise access capability at issue establish not just a circumstantial inference but a direct evidentiary chain connecting Del Gaudio to the misappropriation. (Compl. ¶¶ 30-35, 70.) This evidence is far stronger than the circumstantial patterns found sufficient in *Priority Payment Systems*, where the court credited “a pattern of evidence of its former employees and contractors’ attempts to take the product of their labors” based on email communications, simultaneous employment, and the timing of events. 161 F. Supp. 3d at 1303.

Paradigm Shift’s Misappropriation. Paradigm Shift’s liability is independently established. The GTSA, “by its express terms, extends liability for misappropriation of trade secrets to third parties who receive or benefit from trade secrets acquired by another by improper means.” *Priority Payment Sys.*, 161 F. Supp. 3d at 1302 (citing O.C.G.A. § 10-1-761(2)). As Judge Totenberg held, “[t]he exact nature of Defendants’ relationship with [the misappropriator] is immaterial for

purposes of liability under the GTSA,” and a party “does not absolve [itself] from liability if [it has] knowledge of [the misappropriator’s] conduct and derive[s] a direct economic benefit based on [its] contractual relationship with him.” *Id.*

The same principle applies with equal force under the DTSA. Paradigm Shift published trade secret information that it knew or had reason to know was acquired through improper means. Its own acknowledgment that it coordinated with Apple Product Security before publication confirms that it understood the sensitivity and provenance of the information. (Compl. ¶ 74.) A sophisticated offensive security firm does not come into possession of a detailed BootROM exploit of this nature without knowing its provenance. As Judge Brown observed in a comparable circumstance: “How better to knock off a company’s product than by hiring their key partner (and their key employees) to do it for you?” *Arclin*, No. 1:20-cv-01197, 2020 WL 10056278, at *2 (N.D. Ga. Mar. 31, 2020). Here, how better to replicate a competitor’s proprietary access capability than by hiring the very engineer who helped develop it?

The circumstantial evidence of Paradigm Shift’s knowledge is reinforced by the inference that arises from the nature of the information itself. Just as the court in *Priority Payment Systems* inferred knowledge from the fact that the competitor was developing “a competing merchant management system” using former employees of the plaintiff who had email communications with a contractor who

misappropriated source code on the same day, 161 F. Supp. 3d at 1301-02, the inference of Paradigm Shift’s knowledge here is even stronger: it hired the very engineer who worked on the MSG capability and published a detailed technical blog post describing the same capability under a different name. (Compl. ¶¶ 32-35, 67.)

2. Georgia Trade Secret Misappropriation (GTSA)

The GTSA provides parallel protection. A “trade secret” under the GTSA is information that “(A) Derives economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (B) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.” O.C.G.A. § 10-1-761(4). “Misappropriation” includes “[d]isclosure or use of a trade secret of another without express or implied consent by a person who...at the time of disclosure or use, knew or had reason to know that his or her knowledge of the trade secret was...[a]cquired under circumstances giving rise to a duty to maintain its secrecy or limit its use.” O.C.G.A. § 10-1-761(2)(B)(ii)(II).

For the same reasons set forth above with respect to the DTSA claim, Magnet Forensics is substantially likely to prevail on its GTSA claim. The access capability satisfies the GTSA’s definition of a trade secret, Magnet Forensics took reasonable measures to protect it, and Defendants misappropriated it by publicly disclosing it without authorization and with knowledge of the duty of confidentiality. As the court

found in *Priority Payment Systems*, “computer software programs are trade secrets if the two pronged test is met.” 161 F. Supp. 3d at 1299. The same principle applies with even greater force to a zero-day access capability, which is by definition proprietary, highly specialized, and not publicly known.

3. Breach of Contract

Under Georgia law, a breach of contract claim requires: (1) a valid and enforceable contract; (2) a material breach; and (3) resulting damages. *See McAlister v. Clifton*, 313 Ga. 737, 742 178 (2022). Each element is readily satisfied. The Agreement is a valid, executed contract supported by adequate consideration, including Del Gaudio’s placement with Magnet Forensics, training, access to customers, and access to confidential and proprietary information. (Compl. ¶ 40.) Del Gaudio breached multiple provisions of the Agreement by disclosing Confidential Information and proprietary Materials to Paradigm Shift and the public in violation of Sections 3.1, 3.2, and 5.1, asserting control over Company Inventions and moral rights he had irrevocably assigned and waived under Sections 4.2 and 4.4, and failing to notify Magnet Forensics of the unauthorized use of its Confidential Information as required by Section 5.3. (*Id.* ¶ 140.) The resulting damages include the destruction of the trade secret’s value, harm to competitive position, loss of customer relationships, and the impact on Magnet Forensics’ products and reputation. (Compl. ¶ 109.)

B. Magnet Forensics Will Suffer Irreparable Harm Absent Injunctive Relief

“[A] trade secret[,] once lost, is, of course, lost forever.” *TruTemp Refrigeration & Commercial Climate, LLC v. Mowbray*, No. 1:23-cv-667-ECM, 2023 WL 8004818, at *6 (M.D. Ala. Nov. 17, 2023). Magnet Forensics faces irreparable harm on multiple independent grounds, any one of which independently warrants injunctive relief.

First, the trade secret’s confidentiality is being destroyed in real time. The Publication remains publicly accessible and has been reshared by more than a dozen media outlets in the technology and cybersecurity community. (Compl. ¶ 85.) Each additional day of public availability means additional competitors, researchers, and bad actors gain access to the access capability methodology. This harm cannot be undone because once a trade secret is disclosed, it cannot be restored to its confidential status. *See Arclin*, 2020 WL 10056276, at *10 (finding irreparable harm where confidential information would be “commoditized” and “could not be undone” because employees who learned the information “could not unlearn” it).

Second, the disclosure creates a direct and imminent risk that Apple will patch the zero-day vulnerability in response, rendering the MSG capability permanently valueless. This is not speculative—the Publication identified the vulnerability by name, described the MSG capability methodology in detail, and Paradigm Shift itself acknowledged coordinating with Apple Product Security before publication. If

Apple patches the vulnerability, Magnet Forensics' forensic products will lose critical data access capabilities, directly impacting ongoing law enforcement investigations. (Compl. ¶ 60.) This is the quintessential harm that cannot be compensated with money damages because the MSG capability—the product of years of investment—would be permanently destroyed.

Third, the disclosure enables competitors to replicate Magnet Forensics' proprietary capability without incurring the substantial time and expense that Magnet Forensics invested in developing it. *See Priority Payment Sys.*, 161 F. Supp. 3d at 1303 (finding irreparable harm where “Plaintiffs’ competitive market advantage and customer base from its advanced software system would be diluted” and “[t]he later award of damages would not provide an adequate remedy at law”). Here, the harm is more acute because the MSG capability has already been published to the world—competitors need not even develop a competing product from misappropriated code; they can simply study the publicly available Publication.

Fourth, Magnet Forensics faces irreparable harm to its customer relationships and reputation. Its customers, including law enforcement and intelligence agencies, depend on the absolute confidentiality of these capabilities. Public disclosure undermines customer confidence and jeopardizes ongoing and future business relationships. As Judge Ross found in *SGS*, the disclosure of confidential information to a competitor would cause “irreparable harm, including but not limited

to reputational damage, loss of good will, the potential loss of existing and future client business relationships, loss of market share, and/or loss of a competitive advantage in the marketplace, and a loss of client trust due to the compromised confidential data exposure.” 2025 WL 1779388, at *7.

Fifth, the fact that the trade secret has already been disseminated makes injunctive relief more urgent, not less. Courts in this District have granted emergency relief even where the threat of future disclosure is merely speculative. *See SGS*, 2025 WL 1779388, at *7 (granting preliminary injunction based on threat of disclosure even where defendant had not actually disclosed information to any third party); *Specialty Chem. & Servs., Inc. v. Chandler*, No. 1:87-cv-2338, 1988 WL 618583, at *5 (N.D. Ga. 1988) (“In light of evidence showing that defendants possess a number of [plaintiff’s] trade secrets, the threat of disclosure or use is significant.”). Here, the harm is not merely threatened; it is ongoing and accelerating. The Court can and should act to prevent further dissemination, even if it cannot undo the harm already inflicted.

Finally, Del Gaudio himself acknowledged that breach of the Agreement would cause “serious harm” to Magnet Forensics and agreed that “the Company shall be entitled to specific performance and any injunctive or other equitable relief as a remedy for any such breach.” Agreement §§ 10.2, 10.3. While such contractual

stipulations are not dispositive, they are entitled to significant weight. *See SGS*, 2025 WL 1779388, at *4 (noting contractual stipulation in granting TRO).

C. The Balance of Equities Favors Magnet Forensics

The balance of equities overwhelmingly favors Magnet Forensics. Defendants have no lawful right to possess, use, or publish Magnet Forensics’ trade secrets. The requested injunction requires Defendants only to stop doing what they had no right to do in the first place—disclose another company’s proprietary information. As courts in this District have consistently held, a defendant “cannot suffer compensable harm when enjoined from an unlawful activity.” *Amedisys Holding, LLC v. Interim Healthcare of Atlanta, Inc.*, 793 F. Supp. 2d 1302, 1314 (N.D. Ga. 2011); *see also Priority Payment Sys.*, 161 F. Supp. 3d at 1304 (same); *Sungdo*, 2024 WL 671582, at *1 (same); *Arclin*, 2020 WL 10056278, at *3 (same).

The burden on Defendants is minimal. Taking down a blog post requires nothing more than removing a webpage and associated files. There is no evidence that Defendants will suffer any cognizable harm from complying with their pre-existing legal obligations. As the court found in *Arclin*, “[i]f Defendant ultimately prevails here, the only injury from a preliminary injunction will be some delay.” 2020 WL 10056276, at *10. Here, the “delay” is not even the delivery of a physical product—it is merely the removal of a blog post. The asymmetry could not be more stark.

By contrast, the harm to Magnet Forensics absent an injunction is severe and permanent. The trade secret cannot be undisclosed. Its value diminishes with every hour it remains publicly accessible. If Defendants were allowed to continue their unauthorized disclosure, Magnet Forensics stands to lose not only “significant revenue” but also the “value of its proprietary system [which] will erode materially.” *See Priority Payment Sys.*, 161 F. Supp. 3d at 1304. The balance could not tip more heavily in Magnet Forensics’ favor.

D. The Public Interest Supports Injunctive Relief

The public interest strongly favors injunctive relief. “There is a strong public policy for protecting trade secrets from misappropriation and in promoting fair competition.” *Priority Payment Sys.*, 161 F. Supp. 3d at 1304. Requiring a party to respect its contractual obligations and honor the confidentiality protections it agreed to serves the public interest. *Cunningham Lindsey U.S. LLC v. Box*, No. 1:18-cv-04346-MHC, 2018 WL 6266554, at *10 (N.D. Ga. Oct. 23, 2018) (“The Court finds that the public interest is served by holding parties to a contract they willingly signed.”). And “[i]t is axiomatic that our laws protect private property and set standards for business competition and that obedience to such laws is in the public interest.” *Chandler*, 1988 WL 618583, at *6.

Moreover, there is a “cognizable public interest in discouraging employees from succumbing to the temptation of easy profit by breaching their employer’s trust

and misappropriating proprietary information for their own gain.” *Id.* Denying relief here would send a message that an individual can misappropriate a former employer’s most valuable trade secret, hand it to a competitor, publish it to the world, and face no immediate consequences.

V. CONCLUSION³

For the foregoing reasons, Magnet Forensics respectfully requests that this Court grant its Emergency Motion for Temporary Restraining Order and Preliminary Injunction and enter the Proposed Order submitted herewith.

Date: July 6, 2026

Respectfully Submitted,

TROUTMAN PEPPER LOCKE LLP

By: Moses M. Tincher
Moses M. Tincher
GA Bar No. 578906
600 Peachtree Street NE
Suite 3000
Atlanta, Georgia 30308
(404) 885-2593

³ Magnet Forensics respectfully requests that the Court set the bond at \$1,000, or such other nominal amount as the Court deems appropriate, particularly given that Defendants will suffer no cognizable harm from the injunction and cannot claim injury from being required to comply with their existing legal obligations. Courts in this District routinely set nominal or no bonds in comparable cases. *See, e.g., Arclin*, 2020 WL 10056278, at *3 (setting a nominal bond of \$1,000 for a TRO in a trade secret case); *see SGS*, 2025 WL 1779388, at *8 (waiving the bond requirement entirely).

moses.tincher@troutman.com

Attorneys for Plaintiff
Magnet Forensics, LLC

(Application for admission *Pro Hac*
Vice for Andrea Martin forthcoming)

LOCAL RULE 5.1 CERTIFICATION

I hereby certify that the foregoing has been prepared in Times New Roman 14-point font in accordance with Local Rule 5.1.

This 6th day of July, 2026.

/s/ Moses M. Tincher

Moses M. Tincher
Georgia Bar No. 578906

CERTIFICATE OF SERVICE

This is to certify that I have on this day caused to be electronically filed a true and correct copy of the foregoing with the Clerk of the Court using the CM/ECF system which will automatically send email notification of such filing to all counsel of record. I also hereby certify that on this day I sent the foregoing via overnight mail and electronic mail to the following counsel of record at the address listed below:

Counsel for Defendant Mario Del Gaudio:

Christopher J. Maier
Maier & Maier PLLC
345 South Patrick Street

Alexandria, VA 22314
cjm@maierandmaier.com

Counsel for Defendant Paradigm Shift Technology:

Silvia Saenz de Ormijana
Baker & McKenzie Barcelona, S.L.P.
Av. Diagonal, 652 Edif. D, 8th Floor
Barcelona, Spain 08034
silvia.saenzdeormijana@bakermckenzie.com

This 6th day of July, 2026.

/s/ Moses M. Tincher

Moses M. Tincher
Georgia Bar No. 578906