UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

GATEGUARD, INC.,

Plaintiff,

- against -

AMAZON.COM INC., ET AL.,

Defendants.

21-cv-9321 (JGK)

MEMORANDUM OPINION AND ORDER

JOHN G. KOELTL, District Judge:

The plaintiff, GateGuard, Inc. ("GateGuard"), brought this action against several defendants, Amazon.com Inc., Amazon.com Services, Inc., Amazon.com Services, LLC, and Amazon Logistics, Inc. (collectively, "Amazon"), seeking damages and injunctive relief for various federal and state-law claims arising out of Amazon's alleged pattern of tampering with intercom and access-control devices installed in multifamily residential buildings. As asserted in the First Amended Complaint, GateGuard's state-law claims include trespass to chattels, misappropriation of trade secrets, conversion, tarnishment, unjust enrichment, and tortious interference with existing contractual relations and prospective economic advantage, all in violation of New York law. GateGuard also brings claims under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 et seq., the Lanham Act, 15 U.S.C. § 1125, and the Defend Trade Secrets Act ("DTSA"),

18 U.S.C. § 1832 et seq., and it asserts a putative class claim under the Sherman Antitrust Act, 15 U.S.C. § 1, et seq.

Amazon now moves to dismiss the complaint pursuant to Federal Rule of Civil Procedure 12(b)(6). Amazon also moves to strike GateGuard's class allegations pursuant to Federal Rules of Civil Procedure 12(f) and 23(d)(1)(D). For the reasons below, the motion to dismiss is **granted in part** and **denied in part**, and the motion to strike is **denied** as moot.

I.

Unless otherwise noted, the following facts are taken from the First Amended Complaint ("FAC"), ECF No. 14, and are accepted as true for purposes of the motion to dismiss.[1]

GateGuard is a corporation that develops, manufactures, and sells security technology for multifamily residential properties in New York City and elsewhere. FAC ¶ 2. GateGuard's "flagship" product is an internet-enabled intercom device called "AI Doorman," which can be "seamlessly integrated with a website" that allows authorized users to unlock entrances remotely and to monitor all incoming and outgoing activity. FAC ¶¶ 3, 85; see id. ¶ 88. The device's "unique features" include "face detection and recognition capability," video-chat functionality, data and cloud

[1] Unless otherwise noted, this Memorandum Opinion and Order omits all alterations, omissions, emphasis, quotation marks, and citations in quoted text.

storage, and internet connectivity, among others. Id. ¶¶ 3, 85. These features allow landlords to track prohibited conduct and security risks, id. ¶ 4, and also to "generate real-time logs" of building activity that can be reviewed from any "mobile phone, tablet, or computer," id. ¶ 5; see id. ¶¶ 85, 88.

GateGuard alleges that its AI Doorman device "is built around proprietary technology," id. ¶ 86, which includes "the configuration of its motherboard, the placement and type of electronic circuitry and other components used, the insulation resistance between circuits, the voltages at which the device operates, the mechanisms of internet connectivity, . . . the antennae used[,] . . . the inner casing of the intercom, its system of wall-mounting and hinges, its waterproofing design, and its custom-designed cables," id. ¶ 165. GateGuard allegedly "developed its device[] after thousands of hours of trial and error and years of painstaking research and development," and its "proprietary technology is kept secret from competitors and customers, with only authorized GateGuard agents permitted access to the devices for repairs and troubleshooting." Id. ¶ 166. GateGuard also "possesses a strong and distinctive registered trademark in the name 'GateGuard,'" which GateGuard has "applied" to its intercom devices. Id. ¶ 177.

GateGuard "offers its devices and associated software on a subscription model," pursuant to a "Service Agreement" that each

GateGuard customer is required to execute. Id. ¶ 7; see Service Agmt., Salant Decl., Ex. A, ECF No. 20-1. Under the terms of the Service Agreement, each GateGuard "subscriber" who requests installation of a GateGuard device must pay a security deposit and a one-time "product fee" of $3,699, a heavily discounted fee compared to the "manufacturer's suggested retail purchase price" of $8,649 for the device. FAC ¶ 91. The Service Agreement also grants the subscriber a nonexclusive and nontransferable license to run the software incorporated into GateGuard's devices for a fixed term of years. Id. ¶ 92. All GateGuard subscribers must pay "subscription fees," either on a monthly basis or in the form of a lump sum "prepay[ment]," to make use of GateGuard's software and other services during the contract term. Id. Subscribers are also required to accept certain terms and conditions designed to protect GateGuard's proprietary technology. See id. ¶ 90.

Amazon is a corporate entity with a large presence in the global e-commerce industry. Its business operations include the nationwide shipment and delivery of products sold through its online "marketplace." See, e.g., id. ¶¶ 26, 29, 30-32. In 2019, Amazon allegedly introduced the "Amazon Key for Business" (the "Key"), a "small device" that can be "inserted" into existing intercom systems and "remotely controlled" to provide "Amazon deliverers [with] building access" on a "24/7" basis. Id. ¶¶ 45-

46. GateGuard alleges that Amazon installs the Key at building entrances in one of two ways: sometimes, Amazon connects the Key to a property's existing intercom device using a component called an "extender," id. ¶¶ 46, 108-109, and in other instances, Amazon wires the Key "directly" into the device's "circuitry," id. ¶ 50.

GateGuard alleges that Amazon claims to "seek [building] owner consent" before installing its Keys, but that in practice, Amazon achieves these installations through deceptive means. Id. ¶ 74. For example, Amazon allegedly seeks out "lower-level employees" at a property and urges them to permit a Key installation "quickly," without first contacting building management. Id. ¶¶ 83, 67, 75. GateGuard alleges that in order to persuade building personnel, Amazon will falsely assert that it has already been authorized to carry out the installation, see id. ¶ 50, that the Key is merely an "upgrade to Amazon's delivery system," id. ¶¶ 69, 72-73, or that the Key "will not interfere with [the building's] existing access control system," id. ¶ 82. On some occasions, building staff "relent[]" and allow the installation of a Key, while on others, Amazon allegedly disregards a "firm 'no'" and installs the Key anyway. Id. ¶ 83. GateGuard alleges that in either case, Amazon "tampers with already installed devices" to connect the Key, thereby "enabling Amazon to 'piggy back' on the authorized access granted" to GateGuard, id. ¶ 50, and to "make deliveries into buildings

without resident, superintendent, property manager or third-party control or approval," id. ¶ 80.

GateGuard alleges that Amazon has installed the Key "at over 40 buildings" where GateGuard access systems were already in place, "either without the property owner's consent" or with consent given only in reliance on the alleged misrepresentations described above. Id. ¶ 96. GateGuard "has captured video of Amazon technicians tampering with multiple GateGuard devices," id. ¶ 116, and at one particular property, GateGuard discovered that Amazon had "wedged" an extender into a GateGuard device in order to connect an Amazon Key, id. ¶ 109; see also id. ¶¶ 108-115. GateGuard, "which, under its contract [with customers], has exclusive control over . . . [its] access control devices," did not authorize any of the Key installations involving GateGuard systems. Id. ¶ 104.

GateGuard claims that in many instances, the installation of an Amazon Key has resulted in the damage or destruction of a GateGuard intercom device. Because Amazon allegedly "wire[s]" its Keys "directly into or onto the GateGuard circuitry," the Keys "often short[] the [GateGuard] devices and render[] them inoperable." Id. ¶¶ 50, 106. In one example, Amazon "irreparably destroy[ed] [an] intercom screen" "by wedging [a Key] extender into [a GateGuard device's] case." Id. ¶ 111. GateGuard alleges that the Keys also "interfere with or destroy a building's

primary intercom, electric door locks, and other components." Id. ¶ 79. Building managers have "called GateGuard to repair or replace disabled intercom devices" "[o]n approximately 20 different occasions," id. ¶ 118, and "[e]ach time," GateGuard "has discovered that Amazon tampered with its intercoms," id. ¶ 120. GateGuard alleges that its customers "had no problems" with their intercom systems until "the surreptitious insertion of the [Amazon] Key . . . into GateGuard's device." Id. ¶ 105.

According to GateGuard, "[t]he consequences of Amazon's conduct have been devastating." Id. ¶ 97. Whenever an Amazon Key causes a GateGuard device to malfunction, GateGuard loses "time and money in support and repair." Id. ¶ 118. Moreover, Amazon's conduct has allegedly "damaged [GateGuard's] reputation in the industry," because "GateGuard customers, residents[,] and others have come to believe falsely that GateGuard's intercom systems are defective." Id. ¶¶ 98, 126. GateGuard alleges that when a device malfunctions at one building due to the installation of an Amazon Key, "landlords . . . cancel [GateGuard] contracts covering dozens of additional buildings throughout Manhattan," thereby "multipl[ying]" the damage to GateGuard's business. Id. ¶¶ 101. GateGuard claims to have lost "contracts covering over 110 buildings" and "millions of dollars in . . . revenues" as a "result of Amazon's tactics." Id. ¶ 97.

GateGuard also alleges that, in instances where an Amazon Key does not disable or damage an intercom system, Amazon "has been able to free ride on the GateGuard device" to gain entry into buildings "without paying a royalty or a usage fee." Id. ¶¶ 96-97. Additionally, GateGuard asserts that Amazon is "using GateGuard's proprietary technology to develop certain Key functionalities and to develop a smart intercom of its own," which would "enable" Amazon to "compete with . . . GateGuard" in the "smart building access control market." Id. ¶ 86.

GateGuard claims that it approached Amazon with evidence of its misconduct in October 2020, and Amazon denied responsibility. Id. ¶¶ 125, 130-131. GateGuard alleges that in order to "prevent detection" once GateGuard receives notice of a damaged intercom system, Amazon "removes" its Key from the GateGuard device. Id. ¶ 127. Then, Amazon returns to the property and "surreptitiously reinstall[s]" the Key, or "presents" the Key as an "update" to the existing access control system. Id. ¶¶ 125, 128.

Much of the FAC is devoted to GateGuard's allegations that Amazon carries out the conduct described above in furtherance of "a broader scheme that attempts to monopolize the e-commerce delivery market" and to "dominat[e] . . . nation-wide package delivery." Id. ¶¶ 1, 29, 39, 58. GateGuard estimates that Amazon already controls a substantial share of the national "package shipping market," see, e.g., id. ¶¶ 30, 31-39, and that Amazon

developed the Key to "gain a competitive advantage over all [of its] competitors" in the "e-commerce delivery market" generally, id. ¶¶ 45, 47. In particular, GateGuard claims that by reason of its alleged practice of wrongfully installing Keys into existing residential access-control systems, Amazon is able to outperform its competitors in executing efficient and low-cost "last mile" deliveries. See, e.g., id. ¶¶ 33-34, 47; id. ¶¶ 51-52 ("Amazon's true motivation for deploying the Key . . . [is to] increas[e] the volume and speed of its deliveries into apartment buildings" "without the need to gain entry[.]"); id. ¶¶ 53-54 (Amazon Key gives Amazon "a decisive cost advantage over competitors," who must "spend time and gas circling buildings" and "attempting multiple re-deliveries"); id. ¶¶ 55, 59 (Amazon Key allows "more rapid, reliable deliveries," positioning Amazon to gain "total control of the delivery market" and to "cannibaliz[e]" "Fed Ex" and "UPS"). In short, according to GateGuard, Amazon intends to use the Key as an "essential facility, through which [Amazon] . . . can monopolize" the "e-commerce delivery market" "and, once competitors are driven out of business . . . , raise prices on consumers with no alternative." Id. ¶ 47.

GateGuard commenced this action against Amazon in November 2021, ECF No. 1, and filed the FAC On January 24, 2022. The FAC requests damages and permanent injunctive relief in connection with GateGuard's various federal and state-law causes of action,

and also alleges classwide injury with respect to the federal antitrust claim in particular. On March 10, 2022, Amazon filed its motion to dismiss, ECF No. 18, seeking dismissal of the FAC in its entirety for failure to state a claim.

II.

In deciding a motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6), the Court must accept the allegations in the complaint as true and draw all reasonable inferences in the plaintiff's favor. McCarthy v. Dun & Bradstreet Corp., 482 F.3d 184, 191 (2d Cir. 2007). The Court's function on a motion to dismiss is "not to weigh the evidence that might be presented at a trial but merely to determine whether the complaint itself is legally sufficient." Goldman v. Belden, 754 F.2d 1059, 1067 (2d Cir. 1985).

To survive a motion to dismiss, the complaint "must contain sufficient factual matter, accepted as true, to state a claim for relief that is plausible on its face." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id. While the Court should construe the facts alleged in the light most favorable to the plaintiff, "the tenet that a court must accept as true all of the allegations contained in the complaint is inapplicable to legal conclusions."

Id. Finally, when presented with a motion to dismiss a complaint, the Court may consider documents attached to or referenced in the complaint, documents that the plaintiff either possessed or knew about and relied on in bringing the lawsuit, or matters of which judicial notice may be taken. See Goel v. Bunge, Ltd., 820 F.3d 554, 559 (2d Cir. 2016).[2]

III.

GateGuard asserts its first claim against Amazon under the CFAA, "a criminal statute that also provides a private right of action." Apple Mortg. Corp. v. Barenblatt, 162 F. Supp. 3d 270, 286 (S.D.N.Y. 2016); 18 U.S.C. § 1030(g). The FAC specifically alleges violations of Section 1030(a)(2), which makes it unlawful to "intentionally access[] a computer without authorization" and "thereby obtain[]" "information from any protected computer," 18 U.S.C. § 1030(a)(2)(C), and of Section 1030(a)(5), which makes it

[2] Consistent with these principles, the Court is entitled to consider the GateGuard Service Agreement submitted with Amazon's motion. Although the Service Agreement was not attached to the FAC, GateGuard quotes extensively from it and paraphrases the Service Agreement, see FAC ¶¶ 48, 90-94, provides a hyperlink to the Service Agreement, see id. ¶ 91, and relies on the Service Agreement's terms to establish the essential elements of several claims (including, for example, its tortious interference claims and all claims requiring proof of GateGuard's ownership of its devices). The Service Agreement is therefore integral to the FAC. See Goel, 820 F.3d at 559 ("A document is integral to the complaint where the complaint relies heavily upon its terms and effect."). In any event, the Agreement is subject to judicial notice because it is available online and GateGuard does not dispute its authenticity. See Fed. R. Evid. 201(b); see also Force v. Facebook, Inc., 934 F.3d 53, 59 n.5 (2d Cir. 2019).

unlawful to "intentionally access[] a protected computer without authorization, and as a result," to either "recklessly cause[] damage" or "cause[] damage and loss," id. §§ 1030(a)(5)(B)-(C). In addition to pleading the various elements of these statutory violations, GateGuard must also plausibly allege "loss," as that term is defined in the CFAA, "to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." Id. §§ 1030(c)(4)(A)(i)(I), 1030(g).[3]

Preliminarily, Amazon argues that GateGuard cannot pursue a CFAA claim because GateGuard does not "own" or "control" the intercom devices at issue after their installation. Def.'s Memo. of Law, ECF No. 19, at 11. To support this proposition, Amazon relies in part on statements made and court decisions rendered during a recent criminal proceeding against GateGuard's founder. See id. at 11-12 & n.7. However, it is well understood that while a court can take judicial notice of public court records "in

[3] Section 1030(g) provides that a plaintiff may pursue a civil action under the CFAA only if the alleged violation implicates one of the "factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)," 18 U.S.C. § 1030(g), which includes the "loss" factor paraphrased above, see id. § 1030(c)(4)(A)(i)(I). To the extent GateGuard seeks to rely on the factor concerning "threat[s] to public health or safety," id. § 1030(c)(4)(A)(i)(IV), the FAC lacks specific factual allegations to support that theory of CFAA liability. See FAC ¶ 145. And while GateGuard also appears to invoke the subclause concerning "damage affecting 10 or more protected computers," 18 U.S.C. § 1030(c)(4)(A)(i)(VI), Section 1030(g) does not list that subsection as one of the available grounds for a civil CFAA action. See FAC ¶ 144.

considering a Rule 12(b)(6) motion," the court may do so only "to determine what statements [the records] contained," "not for the truth of the matters asserted." Roth v. Jennings, 489 F.3d 499, 509 (2d Cir. 2007); see also Int'l Star Class Yacht Racing Ass'n v. Tommy Hilfiger U.S.A., Inc., 146 F.3d 66, 70 (2d Cir. 1998). Accordingly, at this stage, the Court cannot credit any argument relying on the contents of statements from the cited criminal proceedings.

Amazon also argues that the terms of GateGuard's Service Agreement clearly contemplate the "sale" of the intercom device to GateGuard's customers, rather than a leasing model in which GateGuard retains ownership of its product. Def.'s Memo. of Law at 11. But a review of the Service Agreement makes plain that this issue cannot be resolved on a motion to dismiss. To support its argument, Amazon points to the Agreement's requirement that customers pay a fixed upfront sum for GateGuard's "Product," see Service Agmt. § 2, and also to a provision stating that "devices which are installed cannot be used elsewhere," id. § 5(B)(ii). However, other terms in the Service Agreement are consistent with GateGuard's position that it merely leases its devices and retains full ownership rights. For example, GateGuard customers are required to pay recurring "subscription fees" for a fixed term of years in order to use the intercom system, id. §§ 1(P), 4(C), and GateGuard repeatedly refers to its products as "our

devices," id. §§ 9(C), 11(A); see also id. § 16(A) (reserving the right to surveil "our systems" after installation). The Agreement also states that the "Product Software" is "licensed, not sold to Subscriber" "during the [subscription] Term," id. § 2(G), and it contains various intellectual-property protections that could be read to preserve GateGuard's ownership rights in its "Products and Services."[4] As these provisions suggest, the language of the Service Agreement is ambiguous with regard to whether GateGuard sells or leases its devices -- and resolving such an ambiguity would require extrinsic evidence of the contracting parties' intent. See Alexander & Alexander Servs., Inc. v. These Certain Underwriters at Lloyd's, London, England, 136 F.3d 82, 86 (2d Cir. 1998).[5] Accordingly, the Court cannot

[4] See, e.g., Service Agmt. § 6(A) ("Subscriber acknowledges any and all Intellectual Property Rights in the Products and Services . . . are and shall remain the property of Provider, and Subscriber shall not . . . question or dispute the ownership thereof by Provider. To the extent Subscriber obtains any rights in the Products or Services or any Intellectual Property Rights therein, Subscriber hereby assigns all of its right, title and interest in and to the same to Provider." (emphasis added)); see also id. § 6(C) ("Except as otherwise specifically permitted under this Agreement . . . , Subscriber shall not . . . use, copy, modify, create derivative works of, distribute, sell, pledge, sublicense, lease, loan, rent, timeshare or provide access to the Products or Services nor permit any third party to do any of the foregoing.").

[5] The same principle would apply under Florida law, which governs the construction of the Service Agreement pursuant to Section 21(E), a choice-of-law provision. See, e.g., Nationstar Mortg. Co. v. Levine, 216 So. 3d 711, 714–15 (Fla. Dist. Ct. App. 2017).

decide the question of GateGuard's ownership rights without a developed evidentiary record.

Turning to the elements of the CFAA claim, Amazon does not dispute that GateGuard's "smart" intercom device, which connects to the internet and features data-collection, video-surveillance, and cloud-storage capabilities, satisfies the CFAA's statutory definition of a "computer." See 18 U.S.C. § 1030(e)(1) (defining "computer" as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions").[6] Rather, Amazon argues that the FAC fails to identify any allegedly accessed computer with sufficient particularity. Def.'s Memo. of Law at 10-11. That argument is meritless. The FAC alleges that Amazon has installed its Key in GateGuard's intercom devices "at over 40 buildings," and that GateGuard has been called to repair allegedly tampered-with devices "[o]n approximately 20 occasions." FAC ¶¶ 96, 118-120. The FAC also provides a detailed example of the purported damage inflicted on a specific GateGuard intercom system after the insertion of a Key, see id. ¶¶ 108-115, and GateGuard alleges

[6] Nor does Amazon dispute that these internet-enabled intercom devices are "protected computers," a term that encompasses any "computer" "used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B); see also Van Buren v. United States, 141 S. Ct. 1648, 1652 (2021) (noting that the definition of "protected computer" in Section 1030(e)(2)(B) covers "all computers that connect to the Internet").

that it has captured surveillance videos of Amazon technicians "tampering with multiple GateGuard devices," id. ¶ 116. These allegations plausibly support an inference that Amazon accessed discrete GateGuard devices, which is all that is required at the pleading stage.

Also unpersuasive is Amazon's argument that its alleged access to GateGuard's devices does not qualify as "intentional[] access[]" within the meaning of the CFAA. See Def.'s Memo. of Law at 13. The Supreme Court recently interpreted "access" in the CFAA context to mean "the act of entering a computer system itself or a particular part of a computer system, such as files, folders, or databases." Van Buren v. United States, 141 S. Ct. 1648, 1657 (2021). The "access" alleged here appears to fit Van Buren's definition. GateGuard claims that Amazon broke open the casing around each device to expose its inner workings, and then either wired its Key directly into the GateGuard circuitry or connected to the device using an "extender" mechanism. See FAC ¶¶ 46, 50, 108-109. The FAC also supports the inference that, by connecting to the GateGuard device, Amazon was able to coopt the device's remote door-opening functionality, enabling Amazon to "free ride" on the operation of GateGuard's computerized system and gain entry into buildings. See, e.g., id. ¶¶ 46, 50, 96,

110. Such alleged conduct constitutes "entering a computer system."[7] Van Buren, 141 S. Ct. at 1657.

The FAC also plausibly alleges that Amazon's "access" to GateGuard's computer systems was "intentional[]" and "without authorization." 18 U.S.C. §§ 1030(a)(2), (5)(B)-(C). GateGuard alleges a specific motive for Amazon's efforts to connect Keys to GateGuard's devices, namely that Amazon is seeking "to give its deliverers direct access" to "apartment lobb[ies]" without any "intervention" from landlords or the intercom provider. FAC ¶¶ 89, 46. The methods that Amazon allegedly employed to access the devices, such as misrepresenting its authority to install a Key or performing the installation secretly, are also indicative of an intent to gain such access. See, e.g., id. ¶¶ 50, 82-83, 99, 96, 105. The FAC's allegations likewise permit an inference that Amazon accessed certain devices "without authorization," meaning

[7] In its reply, Amazon suggests that Van Buren's definition of "access" requires not just entering the computer system, but also "accessing data on the computer." Def.'s Reply, ECF No. 25, at 5 (emphasis in original). But that assertion misreads Van Buren, which makes clear that "entering a computer system itself" is sufficient. 141 S. Ct. at 1657. Amazon's contention that Van Buren relied only on dictionary definitions of "access" that "require the reading, writing, or transferring of 'data'" is inaccurate. Def.'s Reply at 5. Several of those definitions are broader in scope and explicitly encompass access to the "computer system" itself. See Van Buren, 141 S. Ct. at 1657 n.6 (quoting the Oxford English Dictionary, which defines "access" as "to gain access to . . . data, etc., held in a computer or computer-based system, or the system itself," and the Dictionary of Computing, which defines "access" as "to gain entry to data, a computer system, etc." (emphases added)).

"without any permission at all." Van Buren, 141 S. Ct. at 1658; accord United States v. Valle, 807 F.3d 508, 524 (2d Cir. 2015). GateGuard claims that it never gave Amazon permission to access its intercom systems, and that in at least some instances, Amazon accessed a device and installed a Key without the knowledge or consent of building management. See FAC ¶¶ 83, 96, 101, 104.

Moreover, GateGuard adequately pleads that Amazon's alleged misconduct resulted in both "damage" and "loss," two statutorily defined terms that "focus on technological harms -- such as the corruption of files -- of the type unauthorized users cause to computer systems and data." Van Buren, 141 S. Ct. at 1660. The CFAA defines "damage" to mean "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). In this case, GateGuard alleges that Amazon's practice of connecting its Keys to the inner workings of GateGuard's devices caused certain of those devices to "short" or malfunction, sometimes irreparably. FAC ¶¶ 50, 96, 105, 106, 111, 113. Thus, it is reasonable to infer that Amazon's alleged access resulted in damage to some of GateGuard's computer systems, and also in the destruction or impairment of any information or data stored therein. See id. ¶ 106 (alleging that certain devices were "render[ed] . . . inoperable"); id. ¶ 146 (alleging that GateGuard "suffered . . . interference with [its] uploading and preservation of proprietary data"); see also Better Holdco, Inc.

v. Beeline Loans, Inc., No. 20-cv-8686, 2021 WL 3173736, at *3 (S.D.N.Y. July 26, 2021) ("'[D]amage' . . . under [the] CFAA [is] inextricably intertwined with a harm to the computer system itself, its data, or delivery of service.").

The CFAA defines "loss" as follows:

> any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

18 U.S.C. § 1030(e)(11). And both before and after Van Buren, "courts in this District have interpreted the CFAA to require 'loss' related to damage or impairment of the target computer itself." Rekor Sys., Inc. v. Loughlin, No. 19-cv-7767, 2022 WL 789157, at *11 (S.D.N.Y. Mar. 14, 2022). "Thus, for example, a covered loss likely would include costs stemming from efforts to identify, diagnose, or address damage to the protected device or from an interruption of service, and the costs involved in investigating the damage to the computer system." Id. In this case, GateGuard alleges that it has fixed or replaced intercom devices allegedly damaged by a Key on at least 20 occasions, "cost[ing] GateGuard time and money in support and repair." FAC ¶ 118. These alleged costs qualify as "loss" under the CFAA.[8]

[8] It is not clear whether Amazon can be said to have "obtained information" from the GateGuard intercom devices in the course of allegedly accessing those systems, as would be required to

Finally, Amazon argues that GateGuard cannot establish a "loss" in excess of $5,000 arising out of "any single act" of unauthorized computer access. Def.'s Memo. of Law at 12. Relying on GateGuard's product fee of $3,699 and other provisions in the Service Agreement, Amazon estimates that the cost of fully replacing a GateGuard device must be less than $5,000. But both the Service Agreement and the FAC state that the manufacturer's recommended retail price for a GateGuard device is $8,649, which suggests that the cost of replacing even one such device might surpass the $5,000 "loss" threshold. FAC ¶ 91; Service Agmt. § 2(B)-(C). Plainly, a fact question exists as to whether the losses flowing from a single intrusion into a GateGuard device exceeded $5,000, and that question cannot be resolved at this juncture.[9]

---

establish a violation of Section 1030(a)(2). However, because this issue likely implicates a number of fact-intensive and technical questions, it is better addressed at later stages of these proceedings. The Court notes that the question of whether Amazon "obtained information" generally from GateGuard's devices is separate from the question of whether Amazon used GateGuard's proprietary trade secrets to develop its own "smart" technology. Cf. Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) ("The CFAA expressly prohibits improper 'access' of computer information. It does not prohibit misuse or misappropriation."). The latter question arises in connection with GateGuard's trade-secrets claims and is addressed below.

[9] Amazon separately argues that GateGuard cannot plead a "cognizable CFAA injury" based on the "costs incurred to repair malfunctioning devices" because customers must "indemnif[y] GateGuard for such activities" pursuant to the terms of the Service Agreement. Def.'s Memo. of Law at 12 (citing Service

In light of all the above, Amazon's motion to dismiss the CFAA claim is **denied**.

IV.

The FAC also asserts state-law tort claims for conversion, trespass to chattels, tortious interference with contracts, and tortious interference with prospective economic advantage, as well as a claim for unjust enrichment. Both parties assume in their papers that New York law governs these claims, and such "implied consent" suffices "to establish choice of law." Krumme v. Westpoint Stevens, 238 F.3d 133, 138 (2d Cir. 2000).

A.

"A conversion takes place when someone, intentionally and without authority, assumes or exercises control over personal property belonging to someone else, [thereby] interfering with that person's right of possession." Colavito v. N.Y. Organ Donor Network, Inc., 860 N.E.2d 713, 717 (N.Y. 2006). Under New York law, the "[t]wo key elements of conversion are (1) plaintiff's possessory right or interest in the property and (2) defendant's dominion over the property or interference with it, in derogation of plaintiff's rights." Id. In this case, Amazon contends that

---

Agmt. §§ 1(H), 8(A), Sched. A, § 10(B)). But whether GateGuard was actually indemnified or reimbursed for such repairs, and if so, to what extent, are also questions of fact that cannot be resolved on this motion.

GateGuard has failed to state a conversion claim because (1) the FAC does not adequately identify a "specific" device with which Amazon interfered, and (2) GateGuard has not plausibly alleged that it was "completely excluded" from accessing its devices. Def.'s Memo. of Law at 22-24.[10] These arguments are unpersuasive.

First, the FAC identifies the allegedly converted property with sufficient specificity to withstand dismissal. GateGuard alleges that it discovered a Key extender wedged into its device "[a]t one building in Manhattan," FAC ¶ 109, that it has taken videos of Amazon tampering with "multiple GateGuard devices" on other occasions, and that in one such video, "Amazon technicians . . . opened [a] GateGuard device without authorization and destroyed it," id. ¶ 116. The FAC also refers to "20 different" instances in which GateGuard devices malfunctioned due to the installation of a Key. Id. ¶¶ 118, 120. These nonconclusory allegations are enough to sustain an inference that Amazon interfered with particular GateGuard devices.

[10] Amazon also argues that the conversion claim fails because GateGuard has not established legal ownership of the installed intercom devices, and it contends that the trespass to chattels claim discussed below must fail for the same reason. See Def.'s Memo. of Law at 23, 24. However, for the reasons set forth in connection with the CFAA claim, an issue of fact exists as to whether GateGuard retains ownership of its devices even after they are installed at a customer's property, and accordingly, dismissal of the conversion claim or the trespass claim for failure to establish such ownership would be premature.

Second, the fact that GateGuard "maintained access" to the allegedly tampered-with devices does not foreclose GateGuard's conversion claim. Def.'s Memo. of Law at 24. A plaintiff may bring an action for conversion against a defendant whose conduct "amount[ed] to the destruction or taking of the property." Sporn v. MCA Records, Inc., 448 N.E.2d 1324, 1326–27 (N.Y. 1983). In this case, the FAC specifically alleges that Amazon inserted its Keys into GateGuard devices without authorization, and that this conduct destroyed or irreversibly damaged certain of those devices. See FAC ¶¶ 50, 106, 111, 116. These allegations permit an inference that Amazon deprived GateGuard of its rights in at least some of its devices, irrespective of whether GateGuard could "access" its devices after the damage was inflicted.

Thus, Amazon's motion to dismiss GateGuard's conversion claim is **denied**.

B.

Under New York law, the tort of "trespass to chattel occurs when a party intentionally damages or interferes with the use of property belonging to another." Lavazza Premium Coffees Corp. v. Prime Line Distribs. Inc., 575 F. Supp. 3d 445, 474 (S.D.N.Y. 2021). "Interference may be accomplished by (i) dispossessing another of the chattel or (ii) using or intermeddling with [the] chattel." Id. To state a claim for trespass to chattel based on "interference by unauthorized use or intermeddling," a plaintiff

must plausibly allege actual damages flowing from the trespass. Fischkoff v. Iovance Biotherapeutics, Inc., 339 F. Supp. 3d 408, 416 (S.D.N.Y. 2018). In this case, GateGuard adequately alleges (1) interference with its property, in the form of unauthorized use or intermeddling, and (2) actual damages as a result.

The FAC contains nonconclusory allegations that Amazon inserted Keys into the fragile components of GateGuard's devices without consent, for the purpose of capitalizing on the building access that those devices provide. The FAC also alleges that these Key installations caused multiple devices to "short" or "malfunction," sometimes irreparably, see, e.g., FAC ¶¶ 50, 105-106, 108-111, 116-120, and GateGuard describes the alleged damage inflicted on its devices with specificity. See id. ¶ 79 (alleging that Keys can "interfere with or destroy a building's primary intercom, electric door locks, and other components"); id. ¶¶ 111, 113 (explaining how inserting a Key into GateGuard's "incredibl[y] delicate" circuitry causes electrical and physical damage, and citing an example where a Key "destroyed an intercom screen"). These allegations support an inference that Amazon, without authority, intentionally "use[d] or intermeddl[ed] with" GateGuard's property. Lavazza, 575 F. Supp. 3d at 474. They also permit an inference that Amazon's conduct resulted in "harm to the condition, quality, or material value" of at least some of the allegedly tampered-with devices, which is the very sort of

actual injury required to state a trespass to chattels claim. J. Doe No. 1 v. CBS Broad. Inc., 806 N.Y.S.2d 38, 39 (App. Div. 2005); see also Fischkoff, 339 F. Supp. 3d at 416.[11]

Thus, Amazon's motion to dismiss GateGuard's claim for trespass to chattels is **denied.**

C.

"Under New York law, the elements of tortious interference with contract are (1) 'the existence of a valid contract between the plaintiff and a third party'; (2) the 'defendant's knowledge of the contract'; (3) the 'defendant's intentional procurement of the third-party's breach of the contract without justification'; (4) 'actual breach of the contract'; and (5) 'damages resulting therefrom.'" Kirch v. Liberty Media Corp., 449 F.3d 388, 402-03 (2d Cir. 2006) (quoting Lama Holding Co. v. Smith Barney Inc., 668 N.E.2d 1370, 1375 (N.Y. 1996)). GateGuard's FAC pleads sufficient facts to satisfy these elements.

[11] Amazon asserts that GateGuard has failed to satisfy the "actual damages" requirement because the FAC does not "identify a single lost contract or business relationship" flowing from the alleged trespass to chattels. Def.'s Memo. of Law at 24. But the damages inquiry for this specific tort focuses on harm to the quality, condition, or value of the property itself, not on harm to business relationships. Amazon also contends that GateGuard cannot establish actual harm because it is contractually entitled to reimbursement for repairs, but as discussed in connection with the CFAA claim, that argument implicates questions of fact that cannot be resolved at the pleading stage.

Although Amazon argues otherwise, GateGuard's allegations that it executes the Service Agreement with each customer seeking a GateGuard device are specific enough to plead the existence of valid contracts between GateGuard and third parties. See, e.g., FAC ¶¶ 7, 104; id. ¶¶ 91-93 (describing material terms of the Service Agreement). And as GateGuard points out, that Service Agreement forbids customers from allowing others to access or alter those devices without GateGuard's consent. See id. ¶ 166; Service Agmt. § 6(C). The FAC alleges that in light of this restriction, Amazon made false representations to building employees to gain unauthorized and contractually prohibited access to GateGuard devices. See, e.g., FAC ¶ 149 (alleging that Amazon was "aware of these contracts[,] as evidenced by [its] misrepresentation of [its] authority to access and tamper with Gate[G]uard's devices"); id. ¶¶ 50, 96, 99, 104. Accordingly, the FAC permits an inference that Amazon had actual knowledge of the relevant contracts and intentionally procured their breach.[12]

[12] In its reply, Amazon suggests that GateGuard cannot allege any damages based on this theory of tortious interference because the source of GateGuard's claimed injury was "Amazon's allegedly flawed [Key] installation -- not the granting of access." Def.'s Reply at 8. However, GateGuard plausibly alleges that some of its customers canceled their contracts because the insertion of a Key caused the GateGuard device to malfunction, and this alleged loss is a direct and foreseeable consequence of gaining unauthorized access to GateGuard's devices in order to install the Keys. See Rich v. Fox News Network, LLC, 939 F.3d 112, 128 (2d Cir. 2019) (under New York law, "[o]ne who is liable to another for tortious interference with a contract . . . is

Amazon also argues that the Service Agreement "cannot be the basis for a tortious interference claim" because it is an at-will contract. Def.'s Memo. of Law at 20. However, New York courts have allowed plaintiffs to pursue such claims based on "a contract terminable at will" where the defendants used "wrongful conduct," like "fraudulent representations" or "threats," in order to procure the third party's breach. Lowenbraun v. Garvey, 876 N.Y.S.2d 441, 441 (App. Div. 2009) (collecting cases). In this case, the FAC plausibly alleges that Amazon misrepresented its authority to access GateGuard's devices, inducing building staff to allow such access in violation of the Service Agreements.

Thus, Amazon's motion to dismiss the claim for tortious interference with existing contracts is **denied.**

D.

To state a claim for tortious interference with prospective economic advantage under New York law, a plaintiff must plausibly allege that (1) the plaintiff "had a business relationship with a third party," (2) "the defendant knew of that relationship and intentionally interfered with it," (3) the defendant either acted "solely out of malice," or "used dishonest, unfair, or improper means," and (4) "the defendant's interference caused injury to

---

liable for damages for . . . pecuniary loss of the benefits of the contract . . . [and] consequential losses for which the interference is a legal cause").

the relationship." Kirch, 449 F.3d at 400. As with the other tortious interference claim, the allegations in the FAC satisfy these elements.

Amazon contends that the FAC fails to "identify any particular[] existing business relationship with which Amazon intentionally interfered." Def.'s Memo. of Law at 21. However, the FAC plausibly alleges that Amazon was aware of GateGuard's relationships with customers who contracted for the installation of a GateGuard device, that Amazon deliberately gained access to and tampered with those devices even though it lacked authority to do so, and that the resulting damage to many devices caused landlords to cancel contracts not only for the damaged intercom systems, but also for "dozens of additional buildings throughout Manhattan." FAC ¶ 101; see id. ¶ 97 ("When a device malfunctions at one building as a result of Amazon's actions, GateGuard loses the entire portfolio of buildings operated by [the] manager."). These allegations permit the inference that Amazon intentionally interfered in GateGuard's relationships with its customers, and that such interference occasionally resulted in the loss of those relationships and the loss of future contracts for GateGuard.

Amazon's argument that the FAC fails to plead "wrongful" means is likewise unavailing. As a "general rule," a defendant may be held liable for "interference with prospective business relations by wrongful means" only where the conduct at issue

"amount[s] to a crime or an independent tort." Stuart's, LLC v. Edelman, 152 N.Y.S.3d 472, 476 (App. Div. 2021). Additionally, "'[w]rongful means' has been defined to include . . . fraud or misrepresentation." Id. (quoting Carvel Corp. v. Noonan, 818 N.E.2d 1100, 1104 (N.Y. 2004)). The FAC alleges that at least some building employees consented to Amazon's unauthorized Key installation in reliance on Amazon's alleged misrepresentations of its authority to access GateGuard's devices. The FAC also alleges that Amazon used such access to install Keys in a manner that occasionally damaged or destroyed GateGuard's intercom systems -- conduct which, for the reasons outlined above, may constitute an independent tort such as conversion or trespass to chattel.[13]

Accordingly, GateGuard has adequately pleaded its claim for tortious interference with prospective economic relations. The motion to dismiss this claim is **denied.**

[13] In connection with both tortious interference claims, Amazon also relies on statements from the criminal proceedings against GateGuard's founder to argue that the "obvious" cause of the plaintiff's economic injury was not Amazon's alleged misconduct, but GateGuard's earlier failures to fix faulty devices and its mistreatment of customers. Def.'s Memo. of Law at 21-22. For the reasons set forth in connection with Amazon's use of such statements to defend against the CFAA claim, the Court cannot credit these arguments on this motion to dismiss.

E.

Under New York law, "the theory of unjust enrichment lies as a quasi-contract claim . . . rooted in the equitable principle that a person shall not be allowed to enrich himself unjustly at the expense of another." Georgia Malone & Co., Inc. v. Rieder, 973 N.E.2d 743, 746 (N.Y. 2012). To state an unjust enrichment claim, a plaintiff must plausibly allege that (1) the defendant was enriched, (2) at the plaintiff's expense, and (3) "equity and good conscience" do not "permit [the defendant] to retain what is sought to be recovered." Id. Moreover, while "privity" with the defendant is not required, the plaintiff must "assert a connection between the parties that [is] not too attenuated." Id. (citing Mandarin Trading Ltd. v. Wildenstein, 944 N.E.2d 1104, 1111 (N.Y. 2011)). The New York Court of Appeals has provided some guidance on this point, explaining that a relationship is "too attenuated" if the parties were not connected in a manner that "could have caused reliance or inducement," Mandarin, 944 N.E.2d at 1111, or if they "simply had no dealings with each other," Georgia Malone, 973 N.E.2d at 747; see In re Commodity Exch., Inc., 213 F. Supp. 3d 631, 676 (S.D.N.Y. 2016) ("[A]n unjust enrichment claim requires some type of direct dealing or actual, substantive relationship with [the] defendant.").

Amazon persuasively argues that the unjust enrichment claim must be dismissed because the FAC fails to allege a sufficiently

close relationship between Amazon and GateGuard. The thrust of GateGuard's unjust enrichment claim is that Amazon inserts its Keys into already installed devices in order to "free-rid[e]" on GateGuard's existing building-access system. See, e.g., FAC ¶ 187; Pl.'s Opp'n, ECF No. 23, at 21. But GateGuard's theory is that Amazon engages in this practice to gain a competitive edge over GateGuard, and the connection between "competitors . . . is far too attenuated to state a claim in quasi[-]contract." GeigTech East Bay LLC v. Lutron Elecs. Co., Inc., 352 F. Supp. 3d 265, 286 (S.D.N.Y. 2018) (insufficient connection for unjust enrichment where plaintiff alleged that competitor had been "free-riding" on the "use of [p]laintiff's trade dress" at plaintiff's expense). Beyond those allegations, the FAC does not identify any direct dealings between the parties, nor does it point to any course of conduct or communications that could have induced the plaintiff to confer some benefit on Amazon at its own expense. The FAC specifies one interaction in which GateGuard accused Amazon of wrongdoing and Amazon "refused to cease installing [its] Key," FAC ¶¶ 130-134, but it is not plausible that such an exchange could support the existence of a quasi-contractual relationship.

Relying on Mandarin, GateGuard contends that Amazon's "awareness of the injured party can suffice" to establish the requisite relationship for its unjust enrichment claim. Pl.'s Opp'n at 22 (emphasis in original); see Mandarin, 944 N.E.2d at

1111 (dismissing unjust enrichment claim where complaint failed to "indicate a relationship between the parties, or at least an awareness by [the defendant] of [the plaintiff's] existence"). However, the New York Court of Appeals has made plain that the "'awareness' language in Mandarin was dicta," simply "intended to underscore the complete lack of a relationship between the parties in that case," Georgia Malone, 973 N.E.2d at 747 & n.3, and that "mere knowledge . . . is insufficient support a claim for unjust enrichment," id. at 747; see, e.g., NSI Int'l, Inc. v. Horizon Grp. USA, Inc., No. 20-cv-8389, 2021 WL 3038497, at *8 (S.D.N.Y. July 16, 2021) (rejecting argument that defendant's "awareness of how [its] conduct would affect [plaintiff] is enough" to allege sufficient connection). Thus, Amazon's alleged awareness of its "free-riding" on the plaintiff's devices does not give rise to a quasi-contract between the parties.

In any event, "unjust enrichment is not a catchall cause of action to be used when others fail"; the theory applies "only in unusual situations when, though the defendant has not breached a contract nor committed a recognized tort, circumstances create an equitable obligation running from the defendant to the plaintiff." Corsello v. Verizon N.Y., Inc., 967 N.E.2d 1177, 1185 (N.Y. 2012). Thus, "[a]n unjust enrichment claim is not available" if it "simply duplicates, or replaces, a conventional contract or tort claim." Id.; see also Turk v. Rubbermaid Inc., No. 21-cv-

270, 2022 WL 836894, at *14 (S.D.N.Y. Mar. 21, 2022) (collecting cases where unjust enrichment claims were dismissed because they were duplicative of the plaintiff's statutory, contract, or tort claims). In this case, GateGuard's unjust enrichment claim is duplicative of its trade-secret misappropriation claims, which similarly turn on the FAC's allegations that Amazon derives a benefit from its unauthorized free-riding on protected GateGuard technology.[14] Thus, GateGuard cannot recover for unjust enrichment damages on those grounds. See Pauwels v. Deloitte LLP, No. 19-cv-2313, 2020 WL 818742, at *15 (S.D.N.Y. Feb. 19, 2020) (dismissing unjust enrichment claim as "duplicative" because it "hinge[d] on the same facts that provide[d] the basis for the [trade-secret] misappropriation claims").

[14] Compare, e.g., FAC ¶ 167 (alleging, in support of the state-law trade-secrets claim, that Amazon "misappropriated [GateGuard's] trade secrets [and] applied [GateGuard's] intercom devices to [its] own use, [by] accessing the inner workings of [those] devices and installing Key extenders without . . . paying compensation or obtaining consent"), and id. ¶ 166 (GateGuard "developed its devices after thousands of hours of trial and error and years of painstaking research and development"), with id. ¶ 187 (alleging that Amazon was unjustly "enriched by [its] practice of installing the Key . . . inside [GateGuard's] intercom devices without consent by illegally free-riding on the work that [GateGuard] had performed . . . and accessing and misappropriating GateGuard's proprietary technology"), and id. ¶ 188 ("[Amazon's] actions . . . occurred at the expense of [GateGuard] in that [Amazon] profited from [the] development of proprietary technology after several years and thousands of hours of research and development.")

Finally, to the extent GateGuard contends that Amazon benefits when it "causes [GateGuard's] devices to malfunction" because it can then present its Key as an "upgrade," FAC ¶ 188, such alleged conduct does not fit within the framework of unjust enrichment. To state a cognizable unjust enrichment claim, the plaintiff must allege that "it directly conferred a benefit to" or "performed services for" the defendant. NSI Int'l, 2021 WL 3038497, at *8. But the alleged benefit to Amazon here -- the opportunity to present the Key as an "upgrade" to the existing intercom -- does not come about because GateGuard performed some service for Amazon or bestowed that benefit on Amazon directly. Rather, that benefit flows from the damaging consequences of Amazon's alleged affirmative misconduct, namely its tampering with the installed devices. Because the benefit at issue is one that Amazon obtained through its own purported wrongdoing, as opposed to one conferred by the plaintiff, it cannot support an unjust enrichment claim.

In short, the FAC does not allege the sort of relationship required to plead a claim of unjust enrichment. In any event, the unjust enrichment cause of action is duplicative of other claims in this case -- and to the extent it is not, GateGuard fails to plead a cognizable unjust enrichment theory. Therefore, GateGuard's unjust enrichment claim is **dismissed.**

v.

The Court addresses GateGuard's federal and state-law claims for misappropriation of trade secrets together, because "the requirements for showing [the] misappropriation of a trade secret under the DTSA are similar to those for misappropriation under New York law." ExpertConnect, L.L.C. v. Fowler, No. 18-cv-4828, 2019 WL 3004161, at *4 n.1 (S.D.N.Y. July 10, 2019).

To state a trade-secrets misappropriation claim under the DTSA, a plaintiff must plausibly allege that (1) the plaintiff possessed a trade secret, and (2) the defendant misappropriated that trade secret. Id.; 18 U.S.C. § 1836(b)(1). The DTSA defines a "trade secret" as any kind of "financial, business, scientific, technical, economic, or engineering information" that the owner "has taken reasonable measures" to keep secret and that "derives independent economic value . . . from not being generally known to, and not being readily ascertainable through proper means by, another." 18 U.S.C. § 1839(3). Under the DTSA, a trade secret is "misappropriated" where the defendant has either (1) acquired the trade secret by "improper means," such as "theft, bribery, misrepresentation, [or] breach or inducement of a breach of a duty to maintain secrecy," or (2) disclosed or used the trade secret without consent. 18 U.S.C. § 1839(5)-(6); ExpertConnect, L.L.C., 2019 WL 3004161, at *6.

Similarly, to state a trade-secrets misappropriation claim under New York common law, a plaintiff must allege "(1) that [the plaintiff] possessed a trade secret, and (2) that the defendants used that trade secret in breach of an agreement, confidential relationship, or duty, or as a result of discovery by improper means." Faiveley Transp. Malmo AB v. Wabtec Corp., 559 F.3d 110, 117 (2d Cir. 2009). New York law defines a "trade secret" as any "formula, pattern, device or compilation of information which is used in one's business, and which gives the owner an opportunity to obtain an advantage over competitors who do not know or use it." Id. "Improper means" include any "means which fall below the generally accepted standards of commercial morality and reasonable conduct," like making "fraudulent misrepresentations to induce disclosure." Town & Country Linen Corp. v. Ingenious Designs LLC, 556 F. Supp. 3d 222, 255 (S.D.N.Y. 2021).

In determining whether an item qualifies for trade-secret protection, "[t]he most important consideration remains whether the information was secret." Medtech Prods. Inc. v. Ranir, LLC, 596 F. Supp. 2d 778, 787 (S.D.N.Y. 2008). However, "absolute secrecy" is not required; a plaintiff "must show only sufficient secrecy," "meaning that except by use of improper means, there would be difficulty in acquiring the information." Zabit v. Brandometry, LLC, 540 F. Supp. 3d 412, 427 (S.D.N.Y. 2021). In this case, Amazon contends that the "physical components of

GateGuard's devices cannot be trade secrets because they were sold and installed in the public forum," making them "readily accessible" to third parties.[15] Def.'s Memo. of Law at 16-17. Relatedly, Amazon contends that any information "divined" from GateGuard's product was obtained through nonactionable "reverse engineering" of GateGuard's "publicly placed intercoms." Id. at 17. At the pleading stage, these contentions are unpersuasive.

Preliminarily, Amazon's first argument rests on the premise that GateGuard has in fact "sold" its devices for installation in the public forum, thereby relinquishing any proprietary rights in the device and its "design aspects." Id. at 16-17. As Amazon suggests, it is axiomatic that "[b]y definition a trade secret has not been placed in the public domain." Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 484 (1974). But GateGuard alleges that it remains the owner of its devices even after the devices

[15] The alleged trade secrets in this case are "the configuration of [the GateGuard device's] motherboard, the placement and type of electronic circuitry and other components used, the insulation resistance between circuits, the voltages at which the device operates, the mechanisms of internet connectivity, . . . the antennae used[,] . . . the inner casing of the intercom, its system of wall-mounting and hinges, its waterproofing design[,] and its custom-designed cables." FAC ¶ 165. Amazon does not dispute that such items, if kept sufficiently secret, could qualify for trade-secret protection. Moreover, Amazon does not contend that GateGuard failed to plead any of its alleged trade secrets with adequate specificity, as is typically required to state a trade-secrets claim. See Elsevier Inc. v. Dr. Evidence, LLC, No. 17-cv-5540, 2018 WL 557906, at *4 (S.D.N.Y. Jan. 23, 2018).

are installed, see, e.g., FAC ¶¶ 7, 91, 172, and for the reasons set forth with respect to the CFAA claim, the parties' factual dispute as to the truth of these allegations cannot be resolved on a motion to dismiss. Accordingly, it would be premature to endorse any argument that GateGuard's technology lost trade-secret status by virtue of the device's sale.

Moreover, while the intercom devices themselves are placed in building doorways, GateGuard plausibly alleges that it takes reasonable measures to protect the secrecy of each device's inner workings and features, such that those claimed trade secrets can be obtained only through improper means. The FAC alleges that GateGuard "protects its proprietary rights in its devices through [its] Service Agreement and its Terms and Conditions," both of which "must be accepted by all GateGuard customers." FAC ¶ 90. Indeed, the Service Agreement requires GateGuard subscribers to "acknowledge[]" that the device contains GateGuard's "valuable trade secrets," and that "all Intellectual Property Rights in the Products" "are and shall remain [GateGuard's] property." Service Agmt. §§ 6(C), 6(A). The Service Agreement accordingly provides that the subscriber "shall not . . . use, copy, modify, create derivative works of, distribute, sell, pledge, sublicense, lease, loan, rent," "reverse engineer, decompile, disassemble," "or provide access to the Products or Services," "nor permit any third party to do any of the foregoing." Id. § 6(C). GateGuard

also retains and allegedly exercises the right to conduct video surveillance of its intercom systems. Id. § 16(A); see FAC ¶ 116 (alleging that GateGuard has "captured video" of Amazon workers tampering with its devices). Finally, the FAC alleges that "only authorized GateGuard agents [are] permitted access to [installed] devices for repairs and troubleshooting," FAC ¶ 166, and that the trade secrets in its devices cannot otherwise be accessed without "breaking into the GateGuard 'box,'" id. ¶ 86.

In light of the above, the FAC supports an inference that the internal mechanisms of GateGuard's intercom devices are kept sufficiently secret. The design features at issue here are not of the sort that become "easily ascertainable upon inspection once the product is placed on the market." Medtech Prods., 596 F. Supp. 2d at 804; see, e.g., LinkCo, Inc. v. Fujitsu Ltd., 230 F. Supp. 2d 492, 498–99 (S.D.N.Y. 2002) (citing, as examples, a "hotel room design [that] was not a trade secret because it would be publicly disclosed once the hotel room was built, marketed and occupied," and "a window design [that] was not a trade secret where the features were readily apparent from a casual inspection of the . . . window[,] which was available on the open market"). Rather, GateGuard customers and third parties can access the purported trade secrets here only if they break open the casing of a GateGuard device without authorization, defying the various protections that GateGuard has employed to prevent such a result.

Thus, the mere fact that third parties can access the exterior shell of a GateGuard device does not compel a conclusion that GateGuard has placed its trade secrets in the "public domain," and it is not enough to defeat an inference of secrecy at this stage. See, e.g., Uni-Sys., LLC v. U.S. Tennis Ass'n, Inc., 350 F. Supp. 3d 143, 176-77 (E.D.N.Y. 2018) (finding that plaintiff adequately alleged the secrecy of specifications and design techniques for an already installed retractable stadium roof, and noting that although the roof itself "may be visible to the public," the trade secrets "are not"). At most, GateGuard's placement of its devices and the dispute over its ownership raise fact issues as to secrecy, which cannot be resolved on a motion to dismiss.[16] See Medtech Prods., 596 F. Supp. 2d at 787 ("Whether the information was secret is generally a question of fact.").

Also unavailing is Amazon's contention that any trade secrets "divined" from GateGuard's "publicly placed" devices were obtained through "reverse engineering," rendering Amazon's alleged misconduct nonactionable. Def.'s Memo. of Law at 17. Amazon draws this proposition from Kewanee Oil, where the Supreme Court noted that the trade secrets laws "do[] not offer protection against discovery by fair and honest means, such as by . . . so-called

[16] Amazon does not dispute that GateGuard's alleged trade secrets, as described in the FAC, derive independent economic value from their secrecy and confer a competitive advantage on GateGuard.

reverse engineering, that is[,] by starting with a known product and working backward to divine the process which aided in its development or manufacture." 416 U.S. at 476. However, case law postdating Kewanee Oil suggests that a product may be permissibly "reverse engineered" only after its creator has ceded ownership of that product -- by, for example, selling the product on the open market. See, e.g., Roberserve, Ltd. v. Tom's Foods, Inc., 940 F.2d 1441, 1454 (11th Cir. 1991) ("[T]he [state] law of trade secrets cannot protect any unpatented part . . . in the [vending] machine after the machine was sold to [the defendant]. The sale destroyed any reasonable expectation of secrecy by placing the machines in the public domain." (emphasis added)); Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 160 (1989) ("A lock purchaser's reverse engineering of his own lock, and subsequent publication of the serial number-key code correlation, is an example of the . . . reverse engineering expressly allowed by trade secret doctrine." (emphasis added)). And as discussed above, this Court cannot yet discern whether GateGuard remains the owner of its installed devices.

Furthermore, "the term 'reverse engineering' is not a talisman that may immunize the theft of trade secrets"; rather, "[t]he relevant inquiry [is] whether the means used to obtain the alleged trade secret, including reverse engineering, were proper." Telerate Sys., Inc. v. Caro, 689 F. Supp. 221, 233

(S.D.N.Y. 1988); see also Kraus USA, Inc. v. Magarik, No. 17-cv-6541, 2020 WL 2415670, at *6 (S.D.N.Y. May 12, 2020). In this case, the FAC plausibly alleges that GateGuard never authorized Amazon's access to its devices, and that Amazon accessed, tampered with, and wired Keys into GateGuard's technology either (1) without the property owner's knowledge, or (2) upon falsely representing to low-level building employees that such access was permitted. These alleged methods of discovering trade secrets constitute "improper means," whether or not a third party with authorization to access the device could theoretically "reverse engineer" its design. See, e.g., Telerate, 689 F. Supp. at 233 (rejecting defense that plaintiff's software "could have" been "reverse engineered" where defendant wrongfully obtained that software by "connect[ing] [its equipment] to a customer's data line," in violation of the plaintiff's contract with the customer that barred such attachments of third-party equipment).

Finally, Amazon correctly points out the conclusory nature of the FAC's allegation that Amazon has used "GateGuard's proprietary technology to develop certain Key functionalities and to develop a smart intercom of its own." FAC ¶¶ 86, 5. The FAC fails to set forth any facts supporting that allegation. However, GateGuard asserts a second theory of misappropriation, namely that Amazon installs its Keys into GateGuard devices to "piggy back" off of GateGuard's building-access technology. Id.

¶ 50; see id. ¶ 167 (alleging that Amazon "access[ed] the inner workings of the GateGuard devices" and "applied [these] devices to [Amazon's] own use"); Pl.'s Opp'n at 13. Amazon has not cited any authority suggesting that such alleged commandeering of a plaintiff's proprietary technology fails to qualify as "using" or "acquiring" a trade secret under state or federal law. For now, GateGuard's misappropriation claims may proceed past the pleading stage.

Amazon's motion to dismiss GateGuard's federal and state-law claims for misappropriation of trade secrets is **denied**.

VI.

GateGuard brings two claims related to its trademark: an unfair competition claim under the Lanham Act, 15 U.S.C. § 1125(a), and a tarnishment claim under New York's anti-dilution statute, N.Y. Gen. Bus. Law § 360-*l*. Each claim is addressed in turn.

A.

Section 43(a) of the Lanham Act allows the producer of a good or service to bring a civil action against a party who, in connection with a product, "uses in commerce any word, term, name, symbol or device, . . . or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which is likely to cause confusion . . . as to the origin, sponsorship, or approval of [the producer's] goods." 15 U.S.C. § 1125(a)(1). Claims for

unfair competition in violation of Section 43(a) are "governed by a familiar two-prong test," which "looks first to whether the plaintiff's mark is entitled to protection, and second to whether [the] defendant's use of the mark is likely to cause consumers confusion as to the origin or sponsorship of the defendant's goods." Soter Techs., LLC v. IP Video Corp., 523 F. Supp. 3d 389, 397 (S.D.N.Y. 2021). "At its core, an unfair competition claim under the Lanham Act examines whether the public is likely to be misled into believing that the defendant is distributing products manufactured or vouched for by the plaintiff." KatiRoll Co. v. Kati Junction, Inc., 33 F. Supp. 3d 359, 366 (S.D.N.Y. 2014).

The parties do not dispute that the "GateGuard" trademark is federally registered and is sufficiently distinctive to be worthy of protection. Nevertheless, GateGuard's unfair competition claim must be dismissed for failure to satisfy the second prong of the two-part test described above. In support of its claim, GateGuard appears to rely on a theory that Amazon's insertion of Keys into GateGuard-branded devices amounts to unfair competition, because those Key installations often damage GateGuard devices and allow Amazon to present its Key as an "upgrade" to the existing access control system. See Pl.'s Opp'n at 15. But this alleged conduct in no way involves the use of GateGuard's trademark; rather, Amazon is alleged to have made use of GateGuard's hardware and

technology. And while it is true that "any number of activities may be 'in commerce' or create a likelihood of confusion, no such activity is actionable under the Lanham Act absent the 'use' of a trademark." Soter Techs., 523 F. Supp. 3d at 397.

Indeed, the FAC is devoid of any allegations suggesting that Amazon has used GateGuard's trademark in a manner that may create confusion "as to the origin, sponsorship, or approval" of the products at issue. 15 U.S.C. § 1125(a)(1)(A). GateGuard does not allege, for example, that Amazon has used a similar mark to label, promote, or sell the Key, or that Amazon has held out the Key as a GateGuard product. To the contrary, the FAC describes Amazon promotional materials that plainly portray the Key as an Amazon product, and it indicates that the Key bears a distinct "Amazon" label. See, e.g., FAC ¶ 65 (supplying an image of an Amazon Key "Sales Pitch" video conspicuously featuring the Amazon name and logo); id. ¶ 49 (providing a "picture[]" of a typical Key, which is clearly marked with the phrase "[K]ey by [A]mazon"). In short, based on the allegations in the FAC, any inference that Amazon has used the GateGuard mark in a confusing or misleading way is not plausible.[17]

[17] The only allegations suggesting "use" of GateGuard's trademark appear in the FAC's "causes of action" section, where GateGuard asserts, in conclusory fashion, that Amazon "used the GateGuard mark in commerce in connection with the sale or advertising of its Key device," and that Amazon's "use of the mark is likely to cause confusion as to the origin, sponsorship, or approval of

GateGuard also seems to rely on a theory that Amazon's alleged misrepresentations to building managers and employees constitute unfair competition under the portion of Section 43(a) prohibiting "false or misleading description[s] of fact" and "false or misleading representation[s]." 15 U.S.C. § 1125(a)(1). Specifically, GateGuard contends that Amazon presented the Key to building staff "as a necessary intercom 'upgrade,'" while "falsely representing that GateGuard is a device of inferior quality and unreliable for package management." Pl.'s Opp'n at 15. But this specific allegation does not appear in the FAC. Rather, the FAC asserts broadly that "Amazon's strategy is . . . to disparage its competitors' device[s]" before "propos[ing] the Amazon Key as an upgrade," a conclusory assertion lacking any particularized factual allegations to support it. FAC ¶ 122. And to the extent the FAC does cite specific instances in which

---

Amazon's goods." FAC ¶¶ 182, 183. These conclusory allegations cannot cure the FAC's failure to plead particularized facts supporting an inference that Amazon used GateGuard's trademark. See Iqbal, 556 U.S. at 663 ("Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice [to state a claim].")

GateGuard also makes the conclusory allegation that in instances where a Key does not cause a GateGuard device to malfunction, Amazon "profit[s] from GateGuard's . . . brand." FAC ¶ 184. But the FAC does not plausibly allege that Amazon uses GateGuard's brand, name, or trademark to benefit Amazon in any way. Rather, to the extent Amazon profits from its alleged installation of Keys into existing intercom devices, such profits are not the result of GateGuard's "brand," but the result of the access into buildings that the installed intercom devices provide.

Amazon portrayed the Key as an "upgrade," the FAC states that the Key was marketed as an improvement to Amazon's own delivery system. See, e.g., id. ¶¶ 69-70.

Thus, the FAC does not adequately plead a claim under Section 43(a) of the Lanham Act. GateGuard's unfair competition claim is **dismissed.**

B.

New York General Business Law § 360-*l* provides as follows:

> Likelihood of injury to business reputation or of dilution of the distinctive quality of a mark or trade name shall be a ground for injunctive relief . . . notwithstanding the absence of competition between the parties or the absence of confusion as to the source of goods and services.

N. Y. Gen. Bus. Law § 360-*l*. The purpose of this provision is to protect against "dilution," a term referring generally to "the idea that a trademark can lose its ability . . . to clearly and unmistakably distinguish one source [of a product or service] through unauthorized use." Hormel Foods Corp. v. Jim Henson Prods., Inc., 73 F.3d 497, 506 (2d Cir. 1996).

To establish trademark dilution, "two elements must be shown: (1) ownership of a distinctive mark, and (2) a likelihood of dilution." Hormel Foods, 73 F.3d at 606. Moreover, "New York law does not permit a dilution claim" unless the marks at issue (that is, the plaintiff's mark and the mark allegedly used by the defendant) "are substantially similar." Starbucks Corp. v.

Wolfe's Borough Coffee, Inc., 588 F.3d 97, 114 (2d Cir. 2009). One way in which a defendant may "dilute" another's trademark is through "tarnishment," which occurs "when [a mark] is linked to products of shoddy quality, or is portrayed in an unwholesome or unsavory context, with the result that the public will associate the lack of quality or lack of prestige in the defendant's goods with the plaintiff's unrelated goods." Hormel Foods, 73 F.3d at 507. Put differently, "[t]he sine qua non of tarnishment is a finding that plaintiff's mark will suffer negative associations through defendant's use" of the mark. Id.[18]

Here, the tarnishment claim must be dismissed because the FAC fails to allege that Amazon has used a mark "substantially similar" to GateGuard's trademark, which is required to plead a dilution claim under New York law. Starbucks Corp., 588 F.3d at 114. Nowhere in the FAC does GateGuard suggest that Amazon has relied on a mark resembling that of GateGuard to sell the Key, promote the Key, or conduct any other commercial activity with respect to the Key or some different Amazon product. And, without allegations that Amazon has made use of a substantially similar mark, GateGuard cannot plausibly allege that the "plaintiff's

[18] Under New York law, dilution may also occur "by blurring." Starbucks Corp., 588 F.3d at 114. However, GateGuard asserts only a tarnishment claim here. See FAC ¶¶ 176-179.

mark will suffer negative associations through [such] use." Hormel Foods, 73 F.3d at 507.

As with its Lanham Act claim, GateGuard argues that Amazon's "installation [of Keys] can cause the GateGuard device to short," which in turn "deceive[s]" consumers "into believing [that] the GateGuard device is shoddy or inferior to the Key." Pl.'s Opp'n at 14. But this argument is flawed for the reasons discussed above. Although Amazon has allegedly tampered with and exploited GateGuard's technology, this conduct in no way involved the "use" of a mark similar to GateGuard's trademark. Indeed, the Keys themselves feature clear "Amazon" branding, without any markings suggesting an association with GateGuard. See FAC ¶ 49. Thus, while Amazon's alleged misconduct may render certain GateGuard devices "shoddy," that conduct does not amount to tarnishment under New York law.[19] The tarnishment claim is therefore **dismissed.**

[19] In any event, GateGuard's tarnishment claim fails because the FAC does not allege that the "GateGuard" trademark is "registered with the New York Secretary of State," which is a requirement for recovery under New York's trademark protections. Marvel Ent. v. Kellytoy (USA), Inc., 769 F. Supp. 2d 520, 528 (S.D.N.Y. 2011). GateGuard contends that dismissal on these grounds would be "inefficient" because "state registration is in progress." Pl.'s Opp'n at 14 n.5. But even setting aside that a pending trademark application is insufficient as a matter of law, this allegation is absent from the FAC. GateGuard instead supports its assertion with a declaration from its founder. See Teman Decl., ECF No. 23-1, ¶ 8. However, this declaration is not subject to judicial notice, see Fed. R. Evid. 201(b), nor was it attached to,

VII.

GateGuard's final claim is an "attempted monopolization" claim under Section 2 of the Sherman Antitrust Act, which makes it unlawful to "monopolize, or attempt to monopolize . . . any part of . . . trade or commerce." 15 U.S.C. § 2. Amazon argues that this antitrust claim must be dismissed because GateGuard fails to allege a cognizable relevant market and lacks antitrust standing. Dismissal is warranted on each of those grounds.

To plead a claim under the Sherman Act, a plaintiff must (1) define the relevant market, (2) allege an antitrust injury, and (3) allege conduct in violation of the antitrust laws. See Concord Assocs., L.P. v. Ent. Props. Tr., 817 F.3d 46, 52 (2d Cir. 2016). And to prevail on an attempted monopolization claim in particular, "a plaintiff must prove (1) that the defendant has engaged in predatory or anticompetitive conduct with (2) a specific intent to monopolize and (3) a dangerous probability of achieving monopoly power." Spectrum Sports, Inc. v. McQuillan, 506 U.S. 447, 456 (1993). "Establishing a dangerous probability of achieving monopoly power requires proof that the defendant possesses economic power in [the] relevant market." Xerox Corp. v. Media Scis., Inc., 660 F. Supp. 2d 535, 543 (S.D.N.Y. 2009).

---

incorporated by reference into, or integral to the FAC, see Goel, 820 F.3d at 559.

With respect to the meaning of "relevant market," it is a "general rule" that "products constitute part of a single product market if they are 'reasonably interchangeable by consumers for the same purposes,' such that there is high cross-elasticity of demand for the products."[20] Id. (quoting United States v. E.I. du Pont de Nemours & Co., 351 U.S. 377, 380, 395 (1956)). And when a plaintiff "fails to define its proposed relevant market with reference to [this] rule of reasonable interchangeability and cross-elasticity," "the relevant market is legally insufficient and a motion to dismiss may be granted." Chapman v. N.Y. State Div. for Youth, 546 F.3d 230, 238 (2d Cir. 2008).

Here, Amazon persuasively argues that GateGuard has failed to allege a cognizable market definition, a prerequisite to any attempted monopolization claim. GateGuard's "propose[d]" relevant market is the "e-commerce delivery market," Pl.'s Opp'n at 25, which the FAC expressly defines to include the following:

- Third party-logistic ("3PL") providers such as Ship Bob and other fulfillment centers;
- Other package delivery companies — UPS, Fed Ex, USPS, DHL that deliver directly or that work with e-commerce retailers or 3PL providers;
- Other e-commerce retailers that integrate their own delivery solutions or work with other package delivery companies;
- Building access providers with package delivery management functions such as GateGuard;

[20] In antitrust law, "a market has two components: a product market and a geographic market." Concord Assocs., 817 F.3d at 52. Because the parties dispute only the relevant product market, the analysis here is limited to that component.

- Certain landlords who seek to internalize package delivery services, such as external storage, or partner with access providers such as GateGuard.

FAC ¶ 44. The common thread uniting these disparate entities, to the extent one can be discerned, is that each maintains some role or interest in ensuring that products purchased online reach the consumer at home. But this proposed amalgamation of market actors fails to satisfy the rule of reasonable interchangeability. While GateGuard repeatedly emphasizes that its intercom systems provide a "package management" function at the point of delivery, see, e.g., FAC ¶¶ 44, 48-49, it would simply be irrational to infer that consumers would turn to GateGuard's product, a residential intercom device, as an alternative to the package-handling and long-distance shipping services that entities like UPS, FedEx, DHL, and Amazon provide. Although it is more common for courts to reject antitrust claims on the grounds that the proposed market is unduly narrow, "an overly broad product [market] definition may [also] render the alleged product market implausible." In re Set-Top Cable Television Box Antitrust Litig., No. 08-cv-7616, 2011 WL 1432036, at *8 (S.D.N.Y. Apr. 8, 2011), aff'd, 836 F.3d 137 (2d Cir. 2016); see, e.g., Coniglio v. Highwood Servs., Inc., 495 F.2d 1286, 1292 (2d Cir. 1974) (rejecting alleged entertainment market including movies, plays, musicals, and sports exhibitions as "so broadly defined as to render that concept all but meaningless"). That is plainly the case here,

where GateGuard, which nowhere alleges that it sells goods online or transports packages, is lumped into the same market as e-commerce retailers, order-fulfillment centers, and shipping couriers. This "[f]ailure to define the [relevant] market by reference to the rule of reasonable interchangeability is, standing alone, valid grounds for dismissal." Concord Assocs., 817 F.3d at 52.

GateGuard contends that its market definition is viable because participants in the "e-commerce delivery market" compete in distinct "sub-sectors": "fulfillment," "transportation," and "residential access control for package delivery." Pl.'s Opp'n at 25. And GateGuard's antitrust theory is that Amazon deploys wrongful means in the "building access" sub-sector -- that is, the "segment of the market" in which GateGuard participates -- in order to obtain a "decisive competitive advantage over rivals in the transportation and fulfillment segments of the market," where Amazon will be better positioned to drop off packages swiftly and inexpensively. Id. at 26, 27-28; see, e.g., FAC ¶¶ 33-34, 51-59. This theory, however, does not remedy GateGuard's flawed market definition. Instead, it only serves to underscore GateGuard's lack of standing to bring its antitrust claim.

"Antitrust standing is a threshold, pleading-stage inquiry," the purpose of which is to determine "whether the plaintiff is a proper party to bring a private antitrust action." In re Aluminum

Warehousing Antitrust Litig., 833 F.3d 151, 157 (2d Cir. 2016). Accordingly, "when a complaint by its terms fails to establish this requirement[,] [a court] must dismiss it as a matter of law." Id. To demonstrate antitrust standing at the pleading stage, the plaintiff must plausibly allege that (1) "it suffered a special kind of antitrust injury," and (2) "it is a suitable plaintiff to pursue the alleged antitrust violations and thus is an efficient enforcer of the antitrust laws." In re Am. Express Anti-Steering Rules Antitrust Litig., 19 F.4th 127, 138 (2d Cir. 2021). "In order to 'avoid a quagmire,' the Court 'assumes the existence of a violation [of the Sherman Act] in addressing the issue of antitrust standing.'" Harry v. Total Gas & Power N. Am., Inc., 244 F. Supp. 3d 402, 419 (S.D.N.Y. 2017) (quoting Gelboim v. Bank of Am. Corp., 823 F.3d 759, 770 (2d Cir. 2016)), aff'd as modified, 889 F.3d 104 (2d Cir. 2018).

In this case, GateGuard fails to allege that it has suffered an antitrust injury, meaning an "injury [that] is of the type the antitrust laws were intended to prevent." In re Aluminum, 833 F.3d at 157. An antitrust injury is one that tends to "reflect the anticompetitive effect . . . of the [Sherman Act] violation," such as artificially high pricing or reduced output in a particular market. Gelboim, 823 F.3d at 772-73; In re Zinc Antitrust Litig., 155 F. Supp. 3d 337, 362 (S.D.N.Y. 2016) (the "injury resulting from . . . attempted monopolization[] is higher

prices for output or reduced output," meaning "restrictions in availability"). Accordingly, "[c]ompetitors and consumers in the market where trade is allegedly restrained are presumptively the proper plaintiffs to allege antitrust injury." In re Aluminum, 833 F.3d at 157. GateGuard, however, concedes that it does not "compete[] with Amazon in the transportation or shipping of packages for residential delivery," Pl.'s Opp'n at 26, the only market for which the FAC specifically alleges that Amazon might obtain sufficient market power to induce an anticompetitive effect.[21] And while the FAC repeatedly asserts, in conclusory fashion, that Amazon has also inflicted anticompetitive harm in the building-access control market, such an inference cannot reasonably be drawn from the specific facts alleged. Indeed, the FAC is devoid of particularized allegations indicating that

[21] See, e.g., FAC ¶ 30 (Amazon "controls over 20% of the total package shipping market in the United States and shows no sign of showing down"); id. ¶ 31 (Amazon is "already undercutting the big players' average shipping rates by up to 33%," and "Amazon has the potential to decimate UPS and Fed Ex"); id. ¶¶ 30-39 (specific allegations describing Amazon's growing share of the package-shipping market, supported by graphics, citations, statistics, and comparisons to Fed Ex and UPS); id. ¶¶ 28-39 (estimating that Amazon "must control in excess of 60% of all e-commerce deliveries," giving it "the market power to achieve . . . a dominant position in package delivery generally"); id. ¶¶ 54-59 (allegations that the Key allows Amazon to "market a faster, more efficient package delivery service," giving Amazon the means to attain "total control of the delivery market"); id. ¶ 59 (Amazon's "ubiquitous vans and trucks provide a vivid illustration of Amazon's dominant and growing power" over "competitors" like "Fed Ex, UPS").

Amazon has achieved substantial economic power in the building-access control space, much less that Amazon has had an anticompetitive effect in the market for such services.[22] See Harry, 244 F. Supp. 3d at 423 ("[T]he plaintiffs were not

[22] To the contrary, certain of GateGuard's own allegations undercut its assertion that Amazon has stymied competition in the building-access control market, which allegedly encompasses "hundreds of different companies" in New York alone. FAC ¶ 42. For example, the FAC alleges that Amazon's "strategy is not to displace all competitors in the access control market," but rather to "use GateGuard's proprietary technology" in "the longer term" to "develop a 'smart' intercom of its own," FAC ¶ 43 (emphases added), which "will enable [Amazon] to enter the smart building access control market and compete . . . with GateGuard," id. ¶ 86 (emphasis added). Setting aside the wholly speculative nature of the assertion that Amazon is using the plaintiff's trade secrets to develop a "smart" device, these statements necessarily concede that Amazon lacks a competing intercom product of its own and does not currently participate in the building-access control market. Indeed, any argument that Amazon competes directly with GateGuard is inconsistent with GateGuard's descriptions of both the Amazon Key and its own product. GateGuard claims that its "smart" intercom device is a sophisticated piece of building-access technology that allows users to lock and unlock doors remotely, to conduct surveillance of entryways, and to collect data. See, e.g., FAC ¶¶ 3-5, 85-86, 88. Meanwhile, the Amazon Key is alleged to be a "low-tech and simple electronic door key" that must be "wired . . . into" the circuitry of an existing intercom device, id. ¶ 50, and that performs no other function beyond providing access to "Amazon deliverers" in particular, id. ¶¶ 46, 89. These allegations render implausible GateGuard's suggestion that its customers could install a Key as an "upgrade" in lieu of a GateGuard device, see, e.g., FAC ¶ 122, because the Key, as described in the FAC, plainly cannot operate as a substitute for the sort of comprehensive intercom system offered by GateGuard and similar providers. And for the same reason, the FAC's descriptions of GateGuard's product and the Key reinforce the implausibility of any assertion that Amazon has suppressed competition in the building-access control business.

participants in the very market that was directly restrained by the misconduct alleged, and have therefore failed to allege plausibly that . . . they suffered [antitrust injury].").

While GateGuard has alleged that it incurred various injuries -- such as property damage, repair costs, and loss of contracts, customer relationships, and goodwill -- these alleged harms are not the result of stifled competition in the building-access control market. The injuries that GateGuard alleges do not reflect the sort of anticompetitive effects that the Sherman Act was enacted to prevent, and are thus insufficient to support antitrust standing. See Gelboim, 823 F.3d at 772 (an antitrust plaintiff "must prove more than injury causally linked to an illegal presence in the market").

GateGuard also fails to allege that it would be an efficient enforcer of the antitrust laws against Amazon, which is enough on its own to establish that GateGuard "lacks antitrust standing." Gatt Commc'ns, Inc. v. PMC Assocs., L.L.C., 711 F.3d 68, 78 (2d Cir. 2013). To determine whether a private plaintiff would be an efficient enforcer, courts consider the following factors:

> (1) the directness or indirectness of the asserted injury; (2) the existence of more direct victims or the existence of an identifiable class of persons whose self-interest would normally motivate them to vindicate the public interest in antitrust enforcement; (3) the extent to which the claim is highly speculative; and (4) the importance of avoiding either the risk of duplicate recoveries on the one hand, or the danger of complex apportionment of damages on the other.

In re Am. Express, 19 F.4th at 138. "The weight to be given the various factors will necessarily vary with the circumstances of particular cases." Id.

One fundamental problem with GateGuard's antitrust claim is that the FAC does not plausibly allege Amazon's substantial market power in GateGuard's product market -- that is, the market for residential intercom technology. Rather, the FAC's specific allegations of substantial market power focus squarely on Amazon's alleged dominance in the package-shipping market, which is accordingly the relevant market for purposes of evaluating the anticompetitive effect of Amazon's conduct. It is also a market in which GateGuard cannot reasonably claim to compete. To overcome this defect, GateGuard reframes the package-shipping business as part of its proposed "e-commerce delivery market," an expansive and amorphous market encompassing GateGuard and other building-access control providers. But GateGuard cannot rely on a narrowly defined market to establish Amazon's purported market dominance, and then insist on a broadly defined market to cast itself as an Amazon competitor. And because an "efficient enforcer[] would be [a] participant[] in th[e] market" at risk of monopolization, GateGuard is not an efficient enforcer of the antitrust laws in this instance. In re Zinc, 155 F. Supp. 3d at 363; id. at 365 ("Plaintiffs are simply too remote from th[e] [relevant] market

to have antitrust standing to pursue a Section 2 claim based on anticompetitive conduct in that market.").

In any event, even assuming that GateGuard's proposed "e-commerce delivery market" was cognizable and that GateGuard could allege some antitrust injury, the efficient enforcer factors would still require dismissal for lack of antitrust standing. In particular, the second and fourth factors would counsel strongly against allowing GateGuard to proceed with its Sherman Act claim. With respect to the second factor, the most direct victims of Amazon's purported anticompetitive conduct would be package-shipping providers like Fed Ex or UPS, who allegedly lack the ability to compete with Amazon's "last-mile delivery function." FAC ¶ 34; see id. ¶¶ 51-59. These direct competitors represent an "identifiable class . . . whose self-interest would normally motivate them to vindicate the public interest in antitrust enforcement," and accordingly, dismissing GateGuard's Sherman Act claim does not raise any concerns about "leav[ing] a significant antitrust violation undetected or unremedied." In re Am. Express, 19 F.4th at 141. The fact that Amazon's direct competitors have not pursued an antitrust claim similar to the one alleged in this action does not support the recognition of GateGuard's antitrust standing. See Gatt Commc'ns, 711 F.3d at 75. "Instead, it suggests that either the [more direct victims] have been unaware of the [alleged scheme], or, perhaps, that the

facts were other than as alleged by [the] plaintiff." Id.; see also Laydon v. Cooperatieve Rabobank U.A., 55 F.4th 86, 99 (2d Cir. 2022) ("If the 'superior' plaintiff has not sued, one may doubt the existence of any antitrust violation at all.").

Finally, the fourth efficient enforcer factor concerns the risk of "multiple or duplicative recoveries" based on the alleged antitrust violation. Gatt Commc'ns, 711 F.3d at 79. If GateGuard were permitted to seek treble damages for the alleged antitrust violation in this action, the Court could reasonably expect that other participants in GateGuard's sprawling "e-commerce delivery market" -- ranging from "e-commerce retailers" to "third-party logistics providers" to other "[b]uilding access providers," see FAC ¶ 44 -- would claim entitlement to damages based on Amazon's purported misconduct as well. Apportioning damages among this large and diverse pool of prospective antitrust plaintiffs would be exceedingly difficult, and the risks of duplicative recovery would be high.[23] Thus, "allowing the [attempted] monopolization claim would exacerbate the problems that the efficient enforcer concept was meant to resolve." Harry, 244 F. Supp. 3d at 423.

[23] Indeed, the fact that GateGuard seeks to represent a vast and disparate putative class of "package delivery management service providers," "package delivery services, fulfillment centers, e-commerce retailers, and property owners" in connection with its antitrust claim underscores these concerns. FAC ¶ 197.

In short, GateGuard has failed to allege a legally cognizable market definition, a plausible antitrust injury, or status as an efficient enforcer of the antitrust laws. Each of these defects reflects a foundational flaw in GateGuard's antitrust theory: GateGuard does not compete with Amazon in the package-shipping market, the only market for which the FAC sets forth specific, nonconclusory allegations of Amazon's substantial market power. In light of all the above, GateGuard's antitrust claim under Section 2 of the Sherman Act is **dismissed.**

VIII.

Finally, Amazon moves to strike the class allegations in the FAC pursuant to Rules 12(f) and 23(d)(1)(D). GateGuard asserts class allegations only in connection with its antitrust claim. See FAC ¶¶ 195-202. Because that claim has been dismissed from this action, the motion to strike the class allegations is **denied** as moot.

IX.

With respect to GateGuard's claims for tarnishment, unfair competition, unjust enrichment, and violation of the Sherman Act, dismissal with prejudice is warranted. GateGuard already amended its complaint in response to Amazon's pre-motion letter detailing the bases for its anticipated motion to dismiss, and GateGuard has not sought leave to amend again. Under such circumstances, dismissing claims with prejudice is well within the Court's

discretion. See, e.g., City of Pontiac Policemen's & Firemen's Ret. Sys. v. UBS AG, 752 F.3d 173, 188 (2d Cir. 2014); Cruz v. FXDirectDealer, LLC, 720 F.3d 115, 125 (2d Cir. 2013); Warren v. Stop & Shop Supermarket, LLC, 592 F. Supp. 3d 268, 289 (S.D.N.Y. 2022); Marks v. Energy Materials Corp., No. 14-cv-8965, 2015 WL 3616973, at *10 (S.D.N.Y. June 9, 2015). In any event, because an amendment would not cure the fundamental pleading deficiencies identified with respect to each of these claims, granting leave to amend would be futile. See, e.g., Acito v. IMCERA Grp., Inc., 47 F.3d 47, 55 (2d Cir. 1995). Thus, the four claims dismissed from the action are dismissed with prejudice.

CONCLUSION

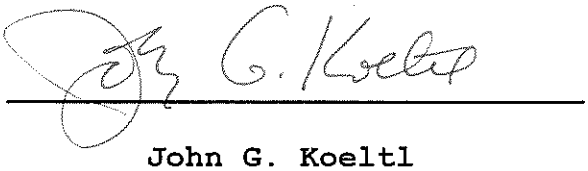
The Court has considered all of the parties' arguments. To the extent not specifically addressed above, those arguments are either moot or without merit. For the foregoing reasons, Amazon's motion to dismiss is **denied** with respect to the following claims in the FAC: computer fraud, in violation of the CFAA, 18 U.S.C. § 1030 et seq. (Count I); tortious interference with existing contracts (Count II); tortious interference with prospective economic advantage (Count III); trespass to chattels (Count IV); conversion (Count V); and misappropriation of trade secrets, in violation of both state law and the DTSA, 18 U.S.C. § 1832 et seq. (Counts VI and VII). Amazon's motion to dismiss is **granted** with regard to GateGuard's claims for tarnishment (Count VIII),

unfair competition in violation of the Lanham Act, 15 U.S.C. § 1125 (Count IX), unjust enrichment (Count X), and attempted monopolization in violation of the Sherman Act, 15 U.S.C. § 1, et seq. (Count XI). These claims are **dismissed with prejudice.** Amazon's motion to strike the FAC's class allegations is **denied** as moot.

The Clerk is respectfully directed to close all pending motions.

SO ORDERED.

Dated: New York, New York
February 16, 2023



John G. Koeltl
United States District Judge