IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

RYANAIR DAC, *Plaintiff*, v. BOOKING HOLDINGS INC., BOOKING.COM B.V., KAYAK SOFTWARE CORPORATION, PRICELINE.COM LLC, and AGODA COMPANY PTE. LTD., *Defendants*.	§ § § § § § § § § § § § §	Civil Action No. 20-1191-WCB **FILED UNDER SEAL**

MEMORANDUM OPINION AND ORDER

The parties have filed motions for summary judgment and motions to exclude expert testimony under *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993). Plaintiff Ryanair DAC ("Ryanair") has moved for summary judgment that defendants Booking.com BV ("Booking.com") and KAYAK Software Corporation ("KAYAK") have violated sections 1030(a)(2)(C) and (a)(5)(C) of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030; for summary judgment on all of Booking.com's counterclaims; and for the exclusion of the testimony of the defendants' experts Timothy O'Neil-Dunne, Jordan Rae Kelly, and Basil Imburgia. Dkt. No. 347. The defendants have moved for summary judgment on all of Ryanair's CFAA claims, Dkt. No. 332, and for the exclusion of the testimony of Ryanair's experts Iain Lopata, Dkt. No. 333, and Anthony Vance, Dkt. No. 334.

I. Background

Ryanair is a low-fare airline based in Ireland that offers flights in Europe and North Africa. Defendants Booking.com, Priceline.com LLC ("Priceline"), and Agoda Company Pte. Ltd.

("Agoda") are online travel companies—also referred to as "Online Travel Agencies," or "OTAs"—that allow consumers to purchase flights, hotel reservations, rental cars, and other travel services. Defendant KAYAK is also an online travel company, but the parties characterize it differently: the defendants characterize KAYAK as a metasearch engine rather than an OTA; Ryanair characterizes KAYAK as an OTA because its users can purchase flights on the KAYAK website, creating bookings referred to by the parties as "facilitated bookings," or via link-out bookings, under which KAYAK customers are offered various third parties, including OTAs, to use to book their flights. Defendant Booking Holdings, Inc., ("BHI") is a holding company whose subsidiaries include Booking.com, Priceline, Agoda, and KAYAK.

Ryanair sells tickets through an online site that lists the flights Ryanair offers and the prices for those flights and ancillary services. That site is freely accessible to the public. Ryanair has implemented a password-protected portion of the website, entitled "myRyanair." To create a myRyanair account, a customer can either sign up with an email and select a password, or sign up with an existing Google, Facebook, or PayPal account. Accounts are generally freely available unless the email domain used for registration is associated with a "blacklist" of domains maintained by Ryanair, in which case the request to create a myRyanair account is denied.

To purchase a ticket on a particular flight, a customer is directed either to create a myRyanair account or to log in to an existing myRyanair account. A customer can select a flight and various ancillary products and services (e.g., a checked bag, trip insurance, etc.) without logging into myRyanair; however, a customer cannot reach the payment page and check out without having a myRyanair account.

During the period at issue in this case, the defendants offered customers the opportunity to purchase Ryanair flights from the defendants' websites. The defendants contracted with vendors

who obtained Ryanair's flight information from Ryanair's website and provided that information to the defendants. The defendants would then display the available Ryanair flights on their websites. If a customer elected to purchase a ticket on one of those flights, the defendants would direct the customer's request to one of the vendors, which would then purchase the ticket and provide the necessary information regarding the booked flight to the customer.

The defendants' information about the available Ryanair flights was obtained mainly through what is referred to as "screen scraping," that is, using programs, often referred to as "bots," that are designed to copy data from the web page's visual interface. Ryanair has accused the defendants of obtaining data from Ryanair's website, either directly or through their vendors, and using that data to sell Ryanair tickets to customers.

Ryanair has objected to the practice of screen scraping and has taken measures to try to prevent it. First, Ryanair has sent cease-and-desist letters to the defendants demanding that they stop the practice. Second, Ryanair has used a program known as "Shield" in an effort to block the defendants and their vendors from obtaining access to Ryanair's websites and from obtaining data from those websites to use in selling Ryanair tickets. Shield uses several strategies to block inquiries from IP addresses that it associates with OTA bot activity. However, Ryanair's efforts to prevent OTAs from accessing the Ryanair website have proved only partially successful.

In 2020, Ryanair filed this action in an effort to prevent further screen-scraping activities by the defendants and parties acting in concert with the defendants. In its complaint, Ryanair premised its claim of liability on the CFAA and sought damages and injunctive relief based on the defendants' alleged violations of that statute. The defendants moved for judgment on the pleadings, and in October 2022 I denied that motion. *See* Dkt. No. 105. The defendants then filed an amended answer and counterclaims charging Ryanair with tortious interference with business

relations, unfair competition, defamation, trade libel, and deceptive trade practices, all related to the disputes over the defendants' activities in accessing the Ryanair website and obtaining flight information from that website.

Following discovery, both sides have filed summary judgment motions directed to various of the claims and counterclaims.

II. Legal Standard

The court "shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a).

On an issue as to which the nonmoving party bears the burden of proof at trial, the party seeking summary judgment "bears the initial responsibility of informing the district court of the basis for its motion, and identifying those portions of 'the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any,' which it believes demonstrate the absence of a genuine issue of material fact." *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986) (quoting Fed. R. Civ. P. 56(c) as of 1986). The burden on the nonmoving party in that situation can be satisfied by "showing," that is, by "pointing out to the district court . . . that there is an absence of evidence to support the nonmoving party's case." *Id.* at 325. If the moving party carries its burden, the nonmovant must "come forward with specific facts showing that there is a genuine issue for trial." *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986) (cleaned up).

On an issue as to which the moving party bears the burden of proof at trial, the party seeking summary judgment must "establish the absence of a genuine factual issue." *Resol. Tr. Corp. v. Gill*, 960 F.2d 336, 340 (3d Cir. 1992). If the motion does not persuasively establish that no factual

issue exists, summary judgment should be denied "even if no opposing evidentiary matter is presented." *Id.* Once the moving party with the burden of proof makes a showing that there is no genuine factual issue, that party is entitled to summary judgment "unless the non-moving party comes forward with probative evidence that would demonstrate the existence of a triable issue of fact." *In re Bressman*, 327 F.3d 229, 238 (3d Cir. 2003); *see Celotex*, 477 U.S. at 322–23; *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 250 (1986).

III. Motions for Summary Judgment on the CFAA Claims

Ryanair has four pending claims under the CFAA:

Count I alleges that all defendants violated section 1030(a)(2)(C), which prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] information from any protected computer."

Count II alleges that all defendants violated section 1030(a)(4), which prohibits "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period."

Count IV alleges that all defendants violated section 1030(a)(5)(B) and (C): section 1030(a)(5)(B) prohibits "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage"; and section 1030(a)(5)(C) prohibits "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage and loss."

Count V alleges that all defendants violated section 1030(b), which prohibits conspiring or attempting to commit a violation of any of the other provisions of section 1030(a).

Ryanair argues that the court should enter summary judgment against defendants Booking.com and KAYAK on counts I and IV on the ground that the evidence conclusively establishes each element of those violations.

For their part, the defendants contend that the court should enter summary judgment against Ryanair on all four counts, for several reasons. With respect to all four counts, the defendants argue: (1) that they have not accessed Ryanair's website in violation of the CFAA; (2) that they are not vicariously liable for the acts of the third-party vendors who have accessed Ryanair's website; (3) that Ryanair cannot establish that the defendants' third-party vendors have accessed Ryanair's website "without authorization," or "in excess of authorization," as required by various paragraphs of subsection 1030(a) of the CFAA; and (4) that Ryanair cannot establish that the defendants have caused $5,000 or more of "loss" to Ryanair in any one-year period, as required by subsection 1030(g) of the CFAA. Regarding Count V, the defendants argue that there is no evidence to support Ryanair's allegation that the defendants are parties to a conspiracy to violate the CFAA, in violation of subsection 1030(b) of the CFAA. And with regard to Count II, the defendants argue that there is no evidence that they had knowing access to information protected by the CFAA or that they acted any point with the intent to defraud in violation of paragraph (4) of subsection 1030(a) of the CFAA.

A. Without Authorization

A critical question regarding the scope of liability under the CFAA is the meaning of the term "without authorization," which appears in several provisions of the statute, including the provisions asserted against the defendants in this case. While determining the meaning of that term might appear to be straightforward, that turns out not to be the case. The Supreme Court addressed the meaning of "authorization" in *Van Buren v. United States*, 593 U.S. 374 (2021), but

even with the benefit of the Supreme Court's guidance in that case, the lower courts have continued to wrestle with the issue.

I addressed the CFAA's conception of authorization in some detail in my order on the defendants' motion to dismiss. *See* Dkt. No. 105 at 21–25. As I explained there, *Van Buren* and its progeny make clear that for an intrusion into a website to be deemed "without authorization," some sort of authentication mechanism (such as the use of a username and password) must be employed to limit access to the website or to a pertinent portion of the website. If the information on the website is publicly available, i.e., if it is not protected by some such authentication mechanism, accessing the website does not violate the statute, even if the access is contrary to the website owner's terms of use governing access to the website or in defiance of a specific directive from the website owner, such as a cease-and-desist letter. *Id.* at 23–24.

Even with that much settled, the parties disagree about how those principles apply to the facts of this case. Ryanair argues that the defendants are not authorized to access any portion of the Ryanair website because Ryanair has erected barriers to access such that the defendants' activities on the Ryanair website are "without authorization" within the meaning of the CFAA. In the alternative, Ryanair argues that the defendants have either acted without authorization or have exceeded the scope of their authorized access to the Ryanair website by accessing the myRyanair portion of the website, which requires the user to open an account and select a password in order to gain access. Dkt. No. 348 at 21–25. The defendants respond that the Ryanair website in its entirety, including the myRyanair portion of the website, is open to the public and that by accessing the website, even against Ryanair's wishes, they are not acting "without authorization" or by "exceed[ing] authorized access." For that reason, the defendants contend that they cannot be held liable for violating any provision of the CFAA. Dkt. No. 335 at 24–27.

i. The Ryanair Website

Ryanair first argues that the defendants are not authorized to access any portion of the Ryanair website because Ryanair has sent cease-and-desist letters to the defendants directing them to stop their screen-scraping activities, and because Ryanair's "Shield" program is designed to block the defendants' bots from gaining access to the website.[1] Ryanair points to [redacted] "endpoints" at which Shield prevents access by unauthorized users. [redacted] *See* Dkt. No. 348 at 22–23. Ryanair argues that by circumventing these authentication mechanisms, the defendants have accessed the website without authorization.

The defendants do not dispute Ryanair's characterization of how Shield operates. Rather, they argue that Ryanair's website is open to the public and that access to the website does not require authorization. Because no authorization is required to access a public website, the defendants contend that any efforts by the website owner to prevent particular users from accessing

[1] The defendants note that for the most part they do not directly access the Ryanair website. Because access to the website is principally done by their contracting partners and others, the defendants contend that they are not liable under the CFAA, either directly or vicariously. I address that argument below. For the purpose of the "without authorization" argument, however, I will assume that the contractors' acts are attributable to the defendants.

such a website "are *bans* of particular users, not authentication mechanisms required to create an authorization framework subject to the CFAA." Dkt. No. 371 at 18. As such, the defendants contend, employing technological measures to block specific users or suspicious activity "does not create an 'authorization' framework absent authentication in the first place." *Id.* at 22. Instead, the defendants argue, there must be an affirmative "code-based authorization framework" to trigger CFAA liability; if a website is open to the public, it is not enough that the website owner purports to create an access restriction through a contractual agreement or term of service. *Id.* at 23.

It is undisputed that any member of the public can freely access the general Ryanair website unless the user's IP address is on Shield's blacklist or the user fails at a Shield endpoint based on the user's behavior, i.e., if Shield identifies the user's behavior as "bot-like." For that reason, whether the user's access is "without authorization" turns on whether Shield's endpoint tests and its blacklist are properly viewed as authentication mechanisms that grant qualifying users access to a private website, as opposed to devices that selectively ban users from a website that is generally open to the public.

The Supreme Court in *Van Buren* used a "gates-up-or-down" metaphor in its analysis of the terms "without authorization" and "exceeds authorized access" in the CFAA. 593 U.S. at 390. As the Court explained, "one either can or cannot access a computer system, and one either can or cannot access certain areas within the system." *Id.* As such, the Court rejected the dissent's contention that "authorization" within the meaning of the CFAA requires "a circumstance-specific analysis." *Id.* at 391 n.10.

Applying the "gates-up-or-down" metaphor used by the Court in *Van Buren*, the Ninth Circuit in *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022), held that a publicly

available webpage has "no gates to lift or lower in the first place," so the concept of access that is without authorization "does not apply to public websites." *Id.* at 1199. The court explained that "[a]uthorization is an affirmative notion, indicating that access is restricted to those specially recognized or admitted." *Id.* at 1195–96. On a publicly available website where "the default is free access without authorization," the court noted, the selective denial of access to some users is best characterized as a ban, not the absence of authorization. *Id*. at 1196.

The facts of *hiQ* are similar to the facts of this case, as applied to the general Ryanair website. The issue in *hiQ* was whether LinkedIn, the professional networking website, could prevent a competitor, hiQ Labs, from collecting and using information that LinkedIn users had shared on their public profiles displayed on LinkedIn's website. Like Ryanair, LinkedIn sent a cease-and-desist letter to hiQ and used anti-bot measures to prevent hiQ from scraping data from LinkedIn's website. The dispute ultimately resulted in litigation. Among the issues before the court was whether hiQ's further scraping and use of LinkedIn's data was "without authorization" within the meaning of the CFAA.

The court viewed the relevant statutory phrase "accesses a computer without authorization" to suggest "a baseline in which access is not generally available and so permission is ordinarily required." *Id.* at 1195. By contrast, the court explained, "[w]here the default is free access without authorization, in ordinary parlance one would characterize selective denial of access as a ban, not as a lack of 'authorization.'" *Id.* at 1196. Again invoking the "gates-up-or-down" metaphor from *Van Buren*, the *hiQ Labs* court concluded that in the case of computers that are not open to the general public, the gates are either up or down depending on whether authorization for access has been given to a particular user. In the case of a computer hosting publicly available webpages,

however, the court concluded that the "computer has erected no gates to lift or lower in the first place," so that "the concept of 'without authorization' does not apply." *Id.* at 1199.

Based on that analysis, the court in *hiQ Labs* rejected LinkedIn's argument that its anti-bot technological measures meant that its websites were not open to the general public. Instead, the court stated that it was likely that "when a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access without authorization under the CFAA." *Id.* at 1201. The court therefore found that LinkedIn's public profiles (i.e., profiles that are visible to a user without the need for the user to be logged in to LinkedIn) do not fall within the reach of the CFAA. *Id.*; *see also Meta Platforms, Inc. v. BrandTotal Ltd.*, 605 F. Supp. 3d 1218, 1262 (N.D. Cal. 2022) ("Where a website is made available to the public without any authentication requirement at least in the first instance, the concept of 'without authorization' does not apply, even if the owner employs technological measures to block specific users, suspicious activity, or—as here—repeated access beyond a particular threshold.") (cleaned up)).

Ryanair urges this court not to adopt the Ninth Circuit's approach in *hiQ Labs*, arguing that the court in *hiQ Labs* construed the CFAA too narrowly and that *hiQ Labs* can be disregarded as an "out-of-circuit" case. Dkt. No. 380 at 8. But the Ninth Circuit's thorough analysis in *hiQ Labs* is convincing, and it is consistent the Supreme Court's treatment of the CFAA in *Van Buren*. Ryanair points to no contrary appellate authority, and instead relies on a district court decision, *CouponCabin LLC v. Savings.com, Inc.*, No. 2:14-CV-39, 2016 WL 3181826 (N.D. Ind. June 8, 2016), which predated both *Van Buren* and *hiQ Labs*. The court in *CouponCabin* defined "without authorization" to mean acting "without formal permission or approval." *Id.* at *3. That court's analysis diverged from the Ninth Circuit's by concluding that a plaintiff can render a user's access

to a public website "without authorization" by notification or by implementing technological measures to block the user. *Id.* at *4.

The legislative history of the CFAA favors the Ninth Circuit's narrower interpretation of the term "authorization." The Ninth Circuit helpfully summarized that history:

> We . . . look to whether the conduct at issue is analogous to "breaking and entering." H.R. Rep. No. 98-894, at 20. Significantly, the version of the CFAA initially enacted in 1984 was limited to a narrow range of computers—namely, those containing national security information or financial data and those operated by or on behalf of the government. *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102, 98 Stat. 2190, 2190–91. None of the computers to which the CFAA initially applied were accessible to the general public; affirmative authorization of some kind was presumptively required.
>
> When section 1030(a)(2)(C) was added in 1996 to extend the prohibition on unauthorized access to any "protected computer," the Senate Judiciary Committee explained that the amendment was designed "to increase protection for the privacy and confidentiality of computer information." S. Rep. No. 104-357, at 7. The legislative history of section 1030 thus makes clear that the prohibition on unauthorized access is properly understood to apply only to private information—information delineated as private through use of a permission requirement of some sort.

hiQ Labs, 31 F. 4th at 1197 (footnote omitted).

At the end of the day, the Ninth Circuit concluded that a business cannot transform a public website into a private one for purposes of the CFAA by implementing a ban on some users based on their perceived use of the website for commercial gain. The court added that the rule of lenity that applies in interpreting criminal statutes favors a narrower interpretation of the term "without authorization," considering that "[t]he statutory prohibition on unauthorized access [applies] both to civil actions and to criminal prosecutions." *Id.* at 1200; *see also Meta Platforms*, 605 F. Supp. 3d at 1260.

Ryanair argues that the Ninth Circuit's interpretation of the CFAA in *hiQ Labs* is inconsistent with other provisions of the statute. In particular, Ryanair argues that the suggestion that authorization means that "access is restricted to those specially recognized or admitted" is at

odds with the proposition that attacks designed to disrupt another computer violate section 1030(a)(5)(A) because "the perpetrators of [such] attacks are never specially recognized or admitted to carry them out, yet they access a protected computer nonetheless." Dkt. No. 380 at 9.

Those propositions are not incompatible. A defendant violates section 1030(a)(5)(A) when he "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." That offense can be committed regardless of whether the defendant was authorized to access the targeted computer. What matters for purposes of section 1030(a)(5)(A) is whether the defendant was authorized to commit one of the specified acts that damaged the protected computer.

Ryanair contends that its Shield program is an affirmative authorization mechanism because Shield monitors every user of Ryanair's website to determine whether the user is authorized based on the user's "Shield score." Dkt. No. 380 at 9 (citing Declaration of John Hemann ("Hemann Decl."), Dkt. No. 343, Exh. 5 at 33:18-35:19; Hemann Decl. Ex. 26 at 83, 91-92; Declaration of Anthony J. Fuga ("Fuga Decl."), Dkt. No. 349, Exh. 5 at 74:27-79:2). That evidence, however, merely confirms that the Ryanair website is open to the public, and that Shield functions not to authenticate qualified users, but to selectively ban users that are perceived as not complying with the terms of use for the Ryanair website.

A decision revoking access to the website for noncompliance with the website's terms of use does not transform the website into a private page under the *hiQ Labs* framework. The defendants are therefore correct that any user can access any page on Ryanair's website without any prior authorization (except for the final payment page of the myRyanair portion of the website). In sum, the defendants' access to the Ryanair website is not "without authorization" as that term is used in the CFAA.

In the following section, I address the authentication argument as it relates to the myRyanair portion of Ryanair's website.

ii. The MyRyanair Portion of the Ryanair Website

Ryanair argues that even if the defendants were not guilty of accessing a protected computer without authorization when they accessed the public Ryanair website, they were guilty of accessing a protected computer without authorization when they gained entry to myRyanair, the private, password-protected portion of the Ryanair website.[2]

Access to myRyanair is required to book a Ryanair flight. *See* Declaration of Iain Lopata ("Lopata Decl."), Dkt No. 350 ¶ 16(c)(iii). Unlike the rest of the Ryanair website, access to the payment page of the myRyanair portion of the website is limited to those who create an account, select a password, and confirm that they have access to the email address associated with their account.[3] In contending that users must be authorized to gain access to the myRyanair website, Ryanair points to what it refers to as two CFAA "gates" that authenticate a user entering the myRyanair portion of the Ryanair website: (1) the requirement to create an account and (2) the requirement that the user log in with a user-selected password. Dkt. No. 348 at 24–25. Account creation involves two hurdles: Ryanair blacklists email domains associated with OTAs and requires verification of the email address used to register, in order to confirm that the user has

[2] Ryanair argues that the defendants' obtaining access to the myRyanair portion of the Ryanair website constitutes "exceed[ing] authorized access" as well as acting "without authorization." Because myRyanair is effectively a separate website, access to the myRyanair portion of the Ryanair website is best analyzed under the "without authorization" provision of the CFAA. In addition, the statute's definition of "exceeds authorized access" requires that the access be used "to obtain or alter information in the computer," 18 U.S.C. § 1030(6), a requirement that is not clearly met in this case.

[3] If the user creates an account through Facebook, Google, or PayPal, as is permitted by the myRyanair website, the email and password associated with the user's account with one of those sources will provide the email and password required to enter the myRyanair payment page.

access to that account. *See* Dkt. No. 348 at 24. Ryanair argues that the account creation, e-mail confirmation, and login requirements are all affirmative methods of authenticating authorized human users and allowing only human users to access the myRyanair portion of the website.[4]

The defendants do not dispute that Ryanair employs those means of enforcing its policy against allowing access to the myRyanair payment page by OTA bots. Instead, they argue that none of those steps qualify as authentication or authorization measures. Dkt. No. 372 at 26–29. The defendants point out that access to a myRyanair account is generally available, in that any user can register by supplying an email address and password, or can bypass the process of providing an email and password by logging in with Facebook, Google, or PayPal credentials. For that reason, the defendants contend, myRyanair, like the rest of the Ryanair website, is public and thus the concepts of "without authorization" or "exceeding authorized access" under the CFAA do not apply. The defendants recognize Ryanair's email domain blacklist as a barrier to account creation but argue that the blacklist is only a ban rather than an authorization scheme. Dkt. No. 372 at 29.

For purposes of the CFAA, the defendants argue that authentication "typically involves a pre-approved list of users that must confirm their identity to access a network." Dkt. No. 335 at 26. The defendants contrast myRyanair, for which a user registers by supplying an email address and password, with Ryanair's company intranet, which requires a username and password issued

[4] Ryanair represents that it recently added a new account verification procedure, which requires customers to provide personal identification to verify that the account holder is who he says he is. Ryanair argued in its briefing that its new account verification procedure is an affirmative method of authenticating human users. In support of its description of the new procedure, Ryanair cited a press release from December 2023. At the hearing on the summary judgment motions, Ryanair conceded that this measure was not in force during the relevant period of this lawsuit. The legal effect of that new verification mechanism is therefore not at issue in this proceeding.

by Ryanair to its employees, who can access the system only with Ryanair's express approval. The defendants argue that only the latter type of authentication mechanism is sufficient to convert what would otherwise be a public website into a private one that would be covered by the "without authorization" or "exceeds authorized access" provisions of the CFAA.

The defendants' characterization of what is required to render a portion of a website "private" is too restrictive. Password-protected systems in which users are free to gain access by signing up for an account and selecting their own passwords could be characterized as quasi-private, in contrast to fully private password-protected systems in which users are assigned a password only after being individually vetted by the website owner. The defendants argue that if a member of the public can create an account and select a password without prior vetting by the website owner, that scenario is not meaningfully different from one in which the member of the public is granted access to the website without creating an account or selecting a password at all.

In fact, however, there is a significant difference between those two scenarios, and the difference bears on whether the access in the second scenario is regarded as unauthorized. When a party is required to create an account and select a password, the website owner potentially has more control over whether to admit the party, particularly if the website owner conditions creation of the account on some kind of verification process, such as Ryanair's requirement of email confirmation. It may be that the verification process is not infallible, but that is merely to say that the party seeking access may be able to obtain unauthorized access by some form of dissembling regarding its identity.

Professor Orin S. Kerr, in his insightful article *Norms of Computer Trespass*, notes that there is a "subtle distinction" between circumventing an IP address ban, which in his view does not violate the CFAA, and a regime in which the computer owner requires an account to access a

computer and then bans that account. In that setting, he argues, circumventing the ban might not be authorized if the context can be interpreted as a complete ban. He explains the difference: "By creating the access control of an account regime, the computer owner takes control of who can access it by making individualized decisions about specific accounts." 116 COLUM. L. REV. 1143, 1177 (2016).

That analysis is consistent with the way courts have interpreted the CFAA. For instance, the court in *Meta Platforms v. BrandTotal Ltd.* granted summary judgment to plaintiff Meta that defendant BrandTotal violated the CFAA when it accessed password-protected areas of Meta's platforms by purchasing or creating Facebook accounts. 605 F. Supp. 3d at 1268. Meta's platforms, like myRyanair's, are not like private intranet pages limited to employees or other designated groups of users. Instead, they are generally open to members of the public, allowing users to register with their own email addresses and passwords.

Similarly, in *hiQ Labs*, the court distinguished hiQ's scraping of public profiles on LinkedIn from the procedure at issue in *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016), in which the defendant gathered information from pages that required a Facebook username and password to obtain access. 31 F.4th at 1199. The court viewed the scraping of public profiles as outside of the "authorization" framework of the CFAA. But the court regarded the username and password requirements as constituting authorization and thus triggering liability under the CFAA when Facebook explicitly revoked authorization.

Reading the Ninth Circuit's decisions in *hiQ Labs* and *Power Ventures* together suggests that the Ninth Circuit regards fully private and quasi-private websites as both being protected by the "without authorization" and "exceeds authorized access" provisions of the CFAA, as opposed to websites that are fully open to the public, which are not subject to those protections. In *hiQ*

Labs, the court characterized *Power Ventures* as a case in which "Power Ventures was gathering user data that was protected by Facebook's username and password authentication system," whereas "the data hiQ was scraping was available to anyone with a web browser." 31 F.4th at 1199. On those facts, the court characterized *Power Ventures* as a case in which "authorization is generally required and has either never been given or has been revoked," whereas in *hiQ Labs*, the information at issue was "presumptively open to all comers." *Id.* Applying that distinction, the password and account creation mechanism used for allowing access to the myRyanair portion of the Ryanair website falls on the *Power Ventures* side of the line.

In another case involving Meta, the court again differentiated between screen scraping data that was publicly available (i.e., that did not require being logged into a Meta platform) and "data behind a log-in screen that is, e.g., password protected." *Meta Platforms, Inc. v. Bright Data Ltd.*, No. 23-CV-00077, 2024 WL 251406, at *5 (N.D. Cal. Jan. 23, 2024).[5] As in the present case, both platforms—Facebook and Instagram—allowed users to register by providing their own emails and passwords. *Id.* at *1. The court specifically differentiated programs designed to defeat screen-scraping mechanisms, such as a CAPTCHA,[6] on an otherwise publicly available website (i.e., where no log-in was required) from a password barrier to a portion of the website. The court concluded that there was a "pivotal" difference between "using CAPTCHA to block automated scraping of public information" and "scraping behind a log-in screen." *Id.* at *7. There, as here, bot-prevention mechanisms on a public website did not transform the public website into a private one. However, by putting a portion of the website (here, the option to check out) behind a log-in

[5] *Bright Data* involved a breach of contract action, not a CFAA action, but it applied a similar "gates-up-or-down" analysis, relying on CFAA case law. *Id.* at *7.

[6] CAPTCHA stands for "Completely Automated Public Turing test to tell Computers and Humans Apart." As the name suggests, such mechanisms are used to differentiate human users from "bots."

mechanism, the website owner limits that portion of its website to those users that it allows to log in.

The defendants are also incorrect in contending that the myRyanair portion of the Ryanair website cannot be private because it does not contain confidential information other than the credit card information that a user inputs. The CFAA is not limited to the protection of private information. While section 1030(a)(2) of the CFAA protects against unauthorized access that results in the intruder obtaining information from a protected computer, other paragraphs of section 1030(a) prohibit unauthorized access without regard to whether the access results in obtaining information.[7] For example, section 1030(a)(4) prohibits unauthorized access with intent to defraud, where the intruder "obtains anything of value," and section 1030(a)(5) prohibits unauthorized access resulting in damage or loss.

Accessing the payment page of the myRyanair portion of the Ryanair website requires authorization. That is, the myRyanair portion of the website uses an authorization scheme that permits some users to create accounts but blocks others. Accessing that portion of the myRyanair website depends on the user being permitted to create an account and then passing a password gate based on having an account. As I noted in my order denying the defendants' motion to dismiss, cease-and-desist letters can withdraw authorization to access a protected portion of a website when an authentication mechanism protects access to that portion of the website. Dkt. No. 105 at 24–

[7] The defendants rely on a statement from the Ninth Circuit's decision in *hiQ Labs* to support their contention that unauthorized access applies only to "private information." *See* Dkt. No. 372 at 21. However, the Ninth Circuit made that statement—that "the prohibition on unauthorized access is properly understood to apply only to private information"—in the context of a discussion of section 1030(a)(2)(c), which requires obtaining information from a protected computer. *See hiQ Labs*, 31 F.3d at 1197. Moreover, the *hiQ Labs* court made clear that information is made private "through use of a permission requirement of some sort." *Id.* In this case, Ryanair makes the checkout process private through use of a permission requirement, and it is the access to a private portion of the website (not private information) that is at issue.

25; *see Facebook*, 844 F.3d at 1199. Accordingly, if the defendants accessed the password-protected portion of the myRyanair website after Ryanair issued cease-and-desist letters to them, they could be found liable for accessing myRyanair "without authorization" within the meaning of 18 U.S.C. § 1030(a).[8] Summary judgment cannot be granted to Ryanair on that issue, however, because factual issues remain as to whether the defendants have accessed the password-protected portion of Ryanair's website, either directly or vicariously, issues that are separately addressed below.

With respect to the defendants' motion for summary judgment, the above discussion leads to the conclusion that any violation of section 1030 would be limited to the unauthorized access to the portion of the myRyanair website that is password protected and requires a user account to access, that is, the payment page of the myRyanair website. As noted, there is no information on that page other than the information input by the user, such as credit card numbers or the like. Therefore, the defendants cannot be held liable for a violation of section 1030(a)(2), which requires not only a showing of unlawful access, but also a showing that the unlawful access resulted in obtaining information from a protected computer. *See* 18 U.S.C. § 1030(a)(2)(C). For that reason, summary judgment is granted to the defendants on Count I of the complaint. In addition, summary judgment is granted to the defendants on Ryanair's conspiracy claim, Count V of the complaint,

[8] That outcome would follow even when the defendants successfully created accounts by using emails that were not on the Ryanair's email domain blacklist. Accounts that are successfully created using email addresses that are not on Ryanair's email domain blacklist and successfully verified through Ryanair's email verification systems are initially made with authorization, in that they are authenticated by Ryanair's two authentication mechanisms. However, after the defendants received cease-and-desist letters, they no longer had authorization to make or use accounts even with emails that are not on the email domain blacklist, because Ryanair could properly revoke authorization to make any account. *See* Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. at 1177 ("[I]f the computer owner requires an account to access a computer and then bans the account, circumventing that ban might not be authorized if the context can be interpreted as a complete ban."); *see also hiQ Labs*, 31 F.4th at 1199.

to the extent that Ryanair relies on the offense set forth in Count I as the offense underlying the conspiracy.

B. Loss

Proof of unauthorized access alone is not enough to support a claim for relief in a private civil action under section 1030. Instead, to sustain any civil claim under the CFAA, a plaintiff must also show that it has "suffer[ed] damage or loss by reason of a violation" of the CFAA. 18 U.S.C. § 1030(g).[9] The nature of qualifying damage or loss is further confined to the types of losses set forth in subclauses I through V of section 1030(c)(4)(A)(i). *Id.* The parties agree that the only relevant factor among those subclauses is the first factor, which requires a showing that the CFAA offense caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value."

A "loss" within the meaning of the CFAA is defined as "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." *Id.* § 1030(e)(11).

In the portion of its motion for summary judgment directed to the issue of loss, Ryanair argues that it has established that both Booking.com and KAYAK have caused Ryanair to suffer losses of more than $5,000 from their screen-scraping activities on the Ryanair website. Dkt No. 348 at 8–16.[10] Ryanair claims a number of expenses as "losses" within the meaning of the CFAA.

[9] Only Ryanair's section 1030(a)(5)(B) and (C) claim (Count IV) requires a showing of both damage *and* loss.

[10] Ryanair does not argue it has suffered more than $5,000 in a single year as a result of the activities of the other defendants.

Those claimed losses include the costs associated with a number of measures Ryanair has employed to try to prevent the defendants and other OTAs from obtaining flight and fare information from Ryanair's website and using it to sell Ryanair tickets to customers. Those expenses include the costs of creating and maintaining technological measures to identify and respond to the defendants' use of automated programs. Such costs, according to Ryanair, include the costs of creating and maintaining the Shield program to detect and blacklist the bots that are used to obtain information and book tickets on Ryanair's website; the costs associated with employing persons to minimize the use of screen-scraping; and the costs of other programs designed to discourage or prevent OTAs from using bots to obtain information from Ryanair's website.

In addition, Ryanair has listed as losses the costs of scaling up its website infrastructure to prevent slowdowns that would otherwise result from the large amount of bot traffic experienced by the Ryanair website. Those costs, according to Ryanair, include the costs of additional servers for making and storing bookings and the costs of creating and maintaining the password-protected portion of myRyanair.

Finally, Ryanair points to the costs of customer verification procedures designed to ensure data integrity relating to customer email and payment methods. Those costs include the costs associated with retaining customer service agents and conducting online customer certification and in-person customer verification.

Ryanair allocates a percentage of the costs of the above measures to Booking.com and KAYAK based on the percentage of bot activity or bookings that Ryanair attributes to each defendant.

In their motion for summary judgment, the defendants argue that for three reasons, Ryanair cannot establish that any violation of section 1030 by any defendant has caused at least $5,000 in losses in any single year. First, the defendants argue that the losses Ryanair cites are attributable to standard website security measures and do not qualify as losses under the CFAA. According to the defendants, a "loss" within the meaning of the CFAA does not include preemptive measures taken to avoid perceived or anticipated problems. Second, the defendants argue that Ryanair has not shown that the defendants have caused any technological harms of the sort that qualify as "losses" under the CFAA. Third, the defendants argue that Ryanair cannot attribute its claimed losses to any one defendant, because it has no reliable allocation methodology. Dkt. No. 335 at 28–35.

i. Losses from investigating and responding to offenses

The parties dispute whether Ryanair can include the costs of securing its websites from the defendants' bots as "losses" under the CFAA. Ryanair argues that measures taken to investigate bot activity, assess damages caused by such bots, and respond to detected bot activity are properly included as losses under the CFAA as part of the reasonable costs of responding to an offense. Dkt. No. 348 at 9–11 (citing *United States v. Nosal*, No. CR-08-0237, 2014 WL 121519, at *5 (N.D. Cal. Jan. 13, 2014); *United States v. Middleton*, 231 F.3d 1207, 1213-14 (9th Cir. 2000); *Zap Cellular, Inc. v. Weintraub*, No. 15-CV-6723, 2022 WL 4325746, at *12 (E.D.N.Y. Sept. 19, 2022)).

The defendants respond that a qualifying "loss" must result from technological harm and that Ryanair has not shown any such harm. Dkt. No. 335 at 27 (citing *Van Buren,* 593 U.S. at 391–92). Rather, the defendants argue, Ryanair's claims of loss focus on preemptive measures designed to prevent technological harm, such as measures to prevent the Ryanair website from

crashing. According to the defendants, those measures cannot be counted as "losses" for purposes of the CFAA, because such measures are prophylactic in nature and are not the results of technical harm to a computer, such as the costs of replacing computer components or reconstituting a database. Dkt. No. 335 at 27–28 (citing *Middleton*, 231 F.3d at 1213; *Univ. Sports Publ'ns Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 388 (S.D.N.Y. 2010); *Brooks v. AM Resorts, LLC*, 954 F. Supp. 2d 331, 338 (E.D. Pa. 2013); *Fink v. Time Warner Cable*, 810 F. Supp. 2d 633, 641 (S.D.N.Y. 2011), *on reconsideration*, 2011 WL 5121068 (S.D.N.Y. Oct. 28, 2011); *Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 474 (S.D.N.Y. 2004), *aff'd*, 166 F. App'x 559 (2d Cir. 2006)).

Prior to *Van Buren*, courts were divided over whether the "cost of responding to an offense" includes the cost of investigating a violation of the CFAA in which a plaintiff does not show that a computer was damaged or that service was interrupted. *Compare Harley Auto. Grp., Inc. v. AP Supply, Inc.*, No. CIV. 12-1110, 2013 WL 6801221, at *6 (D. Minn. Dec. 23, 2013) (CFAA loss requirement is restricted to "actual computer impairment.") (collecting cases); *Jarosch v. Am. Fam. Mut. Ins. Co.*, 837 F. Supp. 2d 980, 1022 (E.D. Wis. 2011) ("costs that are not related to the impairment or damage to a computer or computer system are not cognizable losses under the CFAA"); *Civic Ctr. Motors, Ltd. v. Mason St. Imp. Cars, Ltd.*, 387 F. Supp. 2d 378, 382 (S.D.N.Y. 2005) ("[C]osts not related to computer impairment or computer damages are not compensable under the CFAA."); *Fink*, 810 F. Supp. 2d at 641 (same); *and Nexans Wires S.A.*, 319 F. Supp. 2d at 474–75 (same), *with Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC*, 774 F.3d 1065, 1073–74 (6th Cir. 2014) (treating the costs of investigating unauthorized access to a private website as "loss" under the CFAA); *A.V. ex rel. Vanderhye v. iParadigms*, LLC, 562 F.3d 630, 646 (4th Cir. 2009) (finding the reasonable cost of responding to an offense includes "the

investigation of an offense"); *Nosal*, 2014 WL 121519, at *5–6 (concluding loss does not require "actual damage to a computer system or data"); *and Multiven, Inc. v. Cisco Sys., Inc.*, 725 F. Supp. 2d 887, 895 (N.D. Cal. 2010) ("Costs associated with investigating intrusions into a computer network and taking subsequent remedial measures are losses within the meaning of the statute.").

In *Van Buren v. United States*, the Supreme Court did not squarely address this issue. However, the Court stated that "[t]he statutory definitions of 'damage' and 'loss' . . . focus on technological harms—such as the corruption of files—of the type that unauthorized users can cause to computer systems and data. Limiting 'damage' and 'loss' in this way makes sense in a scheme 'aimed at preventing the typical consequences of hacking.'" 593 U.S. at 391–92 (citation omitted).

Several courts that have addressed the scope of the phrase "cost of responding to an offense" since *Van Buren* have held, based on that language, that a plaintiff cannot rely on the costs of investigating a CFAA violation as constituting a statutory "loss" without showing actual damage to a protected computer or database. *See hiQ Labs*, 31 F.4th at 1195 n.12 (interpreting *Van Buren* as having concluded that the civil remedies section of the CFAA "requires a showing" of technological harm); *Pinebrook Holdings, LLC v. Narup*, No. 4:19-CV-1562, 2022 WL 1773057, at *11 n.17 (E.D. Mo. June 1, 2022); *see also ACI Payments, Inc. v. Conservice, LLC*, No. 121CV00084, 2022 WL 622214, at *12 & n.135 (D. Utah Mar. 3, 2022) (noting a trend towards a restrictive reading of the CFAA, but not deciding which approach applies in that case).

In *Better Holdco, Inc. v. Beeline Loans, Inc.*, for example, the plaintiff alleged that the defendant's employee improperly accessed and downloaded information from the plaintiff's protected computer in violation of the CFAA. No. 20-CV-8686, 2021 WL 3173736, at *3 (S.D.N.Y. July 26, 2021). The plaintiff alleged that it had spent more than $5,000 "responding to"

the CFAA violation. The court, however, interpreted the passage from *Van Buren* discussing the term "loss" to mean that the "cost of responding to an offense" is limited to cases "involving damage to or impairment of the protected computer." *Id.* at *3–4. Because the plaintiff had not alleged that the computer "was damaged or required remediation," the court held that the plaintiff had not stated a claim under the civil remedy provision of the CFAA. *Id.* at *3–4. Other courts in the Southern District of New York have followed *Better Holdco* in that respect. *See William Gottlieb Mgmt. Co., LLC v. Carlin*, No. 20-CIV-08907, 2024 WL 1311854, at *3 (S.D.N.Y. Mar. 26, 2024); *Socialedge, Inc. d/b/a CreatorIQ, v. Traackr, Inc.*, No. 23-CIV-6860, 2024 WL 1533624, at *6 (S.D.N.Y. Apr. 9, 2024).

District courts in other jurisdictions have adopted a broader interpretation of "loss" in the aftermath of *Van Buren*. *See Meta Platforms*, 605 F. Supp. 3d at 1265 (holding that *Van Buren* does not foreclose losses based on "investigative costs" where there has been a violation of the CFAA); *Vox Mktg. Grp. v. Prodigy Promos*, 556 F. Supp. 3d 1280, 1289 (D. Utah 2021) (treating the cost of auditing computers "to determine how Defendants obtained access to them and whether they were compromised in anyway by Defendants" as a "loss" under the CFAA).

Because a "loss" under the CFAA is defined to include "any reasonable cost to any victim, including the cost of responding to an offense," 18 U.S.C. § 1030(e)(8), the term "loss" is best understood to include the cost of an investigation following a CFAA violation, even in instances in which the violation has not resulted in actual impairment of the protected computer or loss of data. Not only is that interpretation faithful to the definition of "loss," but it is consistent with the statutory scheme as a whole, as illustrated by two examples.

First, the offense defined in section 1030(a)(2)(C) covers cases in which a defendant "intentionally accesses a computer without authorization or exceeds authorized access, and thereby

obtains . . . information from any protected computer." That offense does not require proof of actual harm to the protected computer or loss of data. Therefore, if the "cost of responding to" a violation of that provision applies to violations in which there has been no harm to a computer and no loss of data, the cost of responding would have to include incidental costs, such as the cost of investigating the intrusion.

Second, the CFAA contains a separate offense that requires proof that a defendant has "intentionally accesse[d] a protected computer without authorization, and as a result of such conduct, cause[d] damage and loss." 18 U.S.C. § 1030(a)(5)(C). Interpreting the term "loss" to require a plaintiff to show damage to the computer would make the reference to "damage" in the phrase "damage and loss" in that section superfluous.

In *Van Buren*, the Supreme Court drew a contrast between technological harms that are the "typical consequences of hacking" and the "misuse of sensitive information that employees may permissibly access using their computers." *Van Buren*, 593 U.S. at 392 (quotations omitted). The Court pointed to the corruption of computer files as an example of technological harm, but it did not suggest that other harms resulting from unlawful access to protected information would not qualify as "losses" within the meaning of the statute. *See Meta Platforms*, 605 F. Supp. 3d at 1265 ("There is no indication that the *Van Buren* Court would place investigative costs as falling outside the scope of 'the cost of responding to an offense' that the statute specifically incorporates."). Ryanair therefore may include the reasonable costs of investigating and responding to bot traffic by unauthorized users on non-public portions of its website as losses under the CFAA.[11]

[11] The defendants invoke *hiQ Labs* in support of their argument that measures designed to prevent screen scraping do not constitute technological harm and therefore cannot qualify as "losses" for purpose of the CFAA. But *hiQ Labs* held only that screen scraping public information does not qualify as a technological harm. The defendants argue that in that case the plaintiff had alleged that it employed various technological measures to prevent screen scraping and that the

To be sure, there are limits on what a plaintiff may include as the costs of responding to an offense. Because loss must be focused on technological harm, as the Supreme Court said in *Van Buren*, 593 U.S. at 392, the plaintiff may include investigative costs that are "reasonably necessary to respond to the offense, for example by identifying the perpetrator or the method by which the offender accessed the protected information." *Nosal*, 2014 WL 121519, at *5. However, a plaintiff may not include the costs of an investigation that is directed at business harms, such as the costs of investigating how a competitor used protected information obtained as a result of the CFAA violation. Additionally, a plaintiff may include the cost of resecuring its systems after an offense as a loss, but not the cost of measures that make its system more secure than it was before. *See Middleton*, 231 F.3d at 1213.

Applying those standards to Ryanair's various categories of claimed losses, the court concludes as follows:

1. Shield Hosting Costs. Shield is essentially a prophylactic measure designed to prevent screen scraping. Costs of such prophylactic measures are not remedial in nature and therefore do not qualify as "losses" within the meaning of the CFAA. To the extent that the facts at trial show that Shield prevents unauthorized bookings at the payment page after account creation, any portion of those costs allocable to each defendant may qualify as losses under the CFAA for purposes of satisfying the $5,000 threshold requirement for that defendant.

Ninth Circuit did not find the costs of such measures to constitute "losses" under the CFAA. However, the court did not hold that expenses attributable to an unauthorized invasion of a secured website or a secured portion of a website, as alleged in this case, could not constitute "losses" within the meaning of the CFAA.

2. Shield Software Development Costs. Because a plaintiff cannot claim the cost of measures to make a system more secure than it was before as a loss, Ryanair may not include the costs of "developing and updating" Shield, *see* Dkt. 348 at 10, as a "loss" under the CFAA.

3. Business Intelligence Employees. Ryanair attributes two primary roles to its business intelligence employees as related to this action: improving Shield and remedying the harms of bot activity. *See* Fuga Decl. Exh. 15 at 235:6–235:11, 235:22–237:14. For the same reason that it may not include software development costs as a "loss," Ryanair may not include as a "loss" the costs of its business intelligence employees related to developing and improving Shield. However, contingent on proving that bot activity damages the integrity of its data, Ryanair may include the costs entailed in its business intelligence employees' activities relating to remedying the harms of bot activity.[12]

4. New Relic. Ryanair may not include the costs associated with the New Relic software, because that software is used to monitor Ryanair's website, not specifically to respond to or investigate a violation of the CFAA. *See* Fuga Decl. Exh. 5 at 135:4–16.

[12] The defendants argue in a footnote that Ryanair cannot substantiate the costs attributable to its business intelligence and customer service employees. *See* Dkt. No. 335 at 33 n.21 (citing *Glob. Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 642, 651–52 (E.D. Va. 2010). In *Global Policy Partners*, the court held that employee time spent responding to an offense falls within the CFAA's definition of loss. *Id.* at 651. However, the court determined that there was no evidence supporting the assertion that an employee spent 50 hours investigating the alleged CFAA violation beyond conclusory statements that were "so vague that no reasonable jury could conclude that the expended time was reasonably necessary to restore or resecure the system." *Id.* at 651–52. By contrast, in the present case, Ryanair has produced evidence of the functions that the relevant employees perform and an explanation of how the amount of time spent addressing OTA issues was calculated. *See* Declaration of Ji Mao ("Mao Decl."), Dkt. No. 377, Exh. 8 at 3–5; Fuga Decl. Exh. 6 at 28–30, 34–35, 37–38; Fuga Decl. Exh. 14 [Dkt. No. 349-6] at 16:14-19:2, 29:4-33:10. The defendants may, of course, challenge the accuracy of Ryanair's calculations, but at this stage in the proceedings, they have not shown that there is an absence of evidence for those elements of Ryanair's costs.

5. Cloudfront and Amazon Web Application Firewall ("AWS-WAF"). Ryanair may include the costs of Cloudfront and AWS-WAF to the extent that Ryanair can attribute those costs to denying unauthorized booking requests by the defendants. Because both Cloudfront and AWS-WAF have multiple purposes, Ryanair must be able to attribute costs specifically to unauthorized bot activity that violates the CFAA. *See* Fuga Decl. Exh. 5 at 132:6–20 and Fuga Decl. Exh. 15 at 100:10–17 (Cloudfront); Hemann Decl. Exh. 1 at 69:23–29 (Cloudfront); Fuga Decl. Exh. 15 at 38:20–39:11 (AWS-WAF); Hemann Decl. Exh. 1 at 66:13–14, 68:6–10 (AWS-WAF).

6. Navitaire and myRyanair. Ryanair may not include the costs of Navitaire, which provides servers for storing Ryanair bookings, nor the costs of maintaining myRyanair's infrastructure, because those costs are not related to responding to violations, unless the facts developed at trial show that the bot traffic attributable to the defendants has materially increased the cost of Ryanair's server infrastructure.

The defendants argue that the only possible technological harm in this case is the "Monex attack," an event that occurred in 2023 and which Ryanair blames on the defendants. *See* Dkt. No. 335 at 34–35. I address below the question whether the defendants are entitled to summary judgment that they are not liable for the Monex attack. Assuming that Ryanair has made a sufficient showing that the defendants are responsible, at least in part, for the Monex attack, the costs attached to that event would clearly qualify as a "loss" within the meaning of the CFAA, as the loss would be "technological" even under the narrowest interpretation of that term. Ultimately, for the reasons discussed below I conclude that whether a portion of the Monex attack can be attributed to the defendants and whether the Monex attack damaged Ryanair's systems are factual questions that are not suitable for resolution on summary judgment.

ii. Losses attributable to customer verification procedures

Ryanair argues that several costs of verifying customer information are compensable losses related to restoring data under the CFAA. According to Ryanair, the defendants' bots use "fabricated payment methods, passenger personal information, and e-mail addresses when booking flights," resulting in what Ryanair characterizes as "corrupted data." Dkt. No. 348 at 12. Ryanair argues that in order to restore its data integrity it has implemented a variety of costly customer verification procedures. Those measures include the use of customer service agents, an online customer verification procedure, an in-person customer verification procedure, and so-called "digital employees," who communicate with customers who book through OTAs, verify their information for the purpose of issuing refunds, and devise methods of limiting access to the Ryanair website by OTA bots. Ryanair further argues that even if the information was not "fake," the costs to investigate its data integrity would be recognizable as a loss. *Id.* at 13 (citing *Univ. Sports Publ'ns*, 725 F. Supp. 2d at 387).

The defendants argue that none of the costs of Ryanair's online or in-person verification processes constitute losses under the CFAA because they are not actions taken in response to any technological harm, but rather are "self-inflicted business processes" to deter the use of OTAs. Dkt. No. 335 at 33. In particular, the defendants dispute Ryanair's use of the term "corrupted" to refer to the data affected by OTA bookings, arguing that the term is misleading because the customer information is not corrupted, fake, or incorrect. *Id.* at 33 n.23. The defendants further dispute that any "fake" information is given to Ryanair, and that the even for bookings arranged by their vendors, Ryanair ultimately receives the passengers' correct email addresses. Dkt. No. 372 at 33–34. And even if the information was "incorrect," the defendants assert that the data was

not "corrupted" in the technical sense of that term, but rather is, at most, "lacking from a business analytics perspective." *Id.* at 6.

Genuine issues of material fact preclude summary judgment for either side on this issue. First, the question whether the OTA bookings affect the integrity of Ryanair's data turns on whether the bookings were unauthorized. If Ryanair is correct in its theory of the case, the unauthorized bookings affect Ryanair's data integrity because such bookings input information into Ryanair's database that never should have been there in the first place. Second, there is a question whether Ryanair's verification measures are directed at data integrity or were simply a business practice designed to discourage the use of OTAs is a contested factual issue. Third, whether the OTAs' customer details and payment methods are in fact "fake" is also contested. In fact, it is the basis of the counterclaims addressed *infra* section IV.A.

iii. Ryanair's allocation method

The defendants argue that even if Ryanair's alleged losses are compensable under the CFAA, the court must enter summary judgment for the defendants because Ryanair cannot attribute $5,000 or more of loss in a single year to any defendant. Dkt. No. 335 at 35; Dkt. No. 372 at 8–9**.**

The defendants argue that Ryanair conceded this issue as it applies to defendants Agoda, Priceline, and BHI based on the report of Ryanair's expert, Iain Lopata. *See* Hemann Decl. Exh. 40 ¶¶ 161, 176–182. Ryanair responds that Mr. Lopata merely stated he could not calculate the percentage of OTA bookings attributed to those defendants. *See* Dkt. No. 376 at 31.

The defendants mischaracterize the report as a concession. In paragraph 161 of his report, Mr. Lopata concluded that if BHI is found liable for conspiring with the other defendants, BHI would be liable for at least the costs attributable to Booking.com. In paragraphs 176 through 182,

Mr. Lopata explained that he could not calculate the percentage of total OTA bookings attributable to either Agoda or Priceline because at that point he had not received information as to how many bookings had been made via the link-out method. That does not establish that, if Ryanair introduces evidence as to the number of bookings attributable to those defendants, Ryanair cannot allocate a pro-rata share of costs to those bookings.[13]

The defendants next argue that Ryanair cannot meet the $5,000 threshold even for defendants Booking.com and KAYAK because Ryanair includes costs associated with basic web security and business costs. This issue is addressed in the discussion of which costs Ryanair may include as losses above: Ryanair may include only the costs above and the defendants have not shown definitively that those costs will not add up to at least $5,000.

Finally, the defendants argue that Ryanair's expert Mr. Lopata used an unreliable method to attribute costs to the defendants because he failed to follow appropriate principles for calculating damages and failed to provide sufficient support for the calculation of percentages of OTA bookings attributable to each defendant. The defendants rely largely on their motion for the exclusion of Mr. Lopata's testimony to support this argument. In responding, Ryanair similarly relies on its response to that *Daubert* motion. This issue is addressed in greater detail, in section VI.A, *infra*. For the purposes of summary judgment on the issue of loss, however, it suffices to say that the defendants have not met their burden of showing that Ryanair will be unable to allocate permissible costs, as defined by the court, to each of the defendants by introducing evidence at trial as to the bookings that are attributable to each defendant.

[13] Ryanair argues in its response that all annual costs of Shield are attributable to each defendant individually. *See* Dkt. No. 376 at 31. This is incorrect; Ryanair must be able to apportion the chargeable costs of Shield to each defendant individually.

In sum, while some of the costs that Ryanair describes as losses under the CFAA are beyond the statutory definition of "loss," other costs fall within that definition. Based on the record at present, the defendants have not shown that Ryanair will be unable to establish a loss of at least $5,000 attributable to each defendant. However, because Ryanair's loss calculations include some costs that are excluded by the CFAA and some of its listed costs are disputed, it is also the case that Ryanair has not established conclusively that defendants Booking.com and Kayak have each caused Ryanair at least $5,000 in losses in any one-year period. Accordingly, both parties' motions for summary judgment on the issue of loss are denied.

C. Direct Liability

The defendants argue that none of the defendants are directly liable for any of the claimed CFAA violations because no defendant directly accesses Ryanair's website to obtain Ryanair flight information or to book Ryanair flights. Dkt. No. 335 at 17–18. Ryanair responds that at least KAYAK has admitted to accessing the Ryanair website without authorization to confirm the accuracy of flight information that its third-party vendors scrape from the website. Dkt. No. 376 at 7 (citing Mao Decl. Exh. 5 at 225:2-25). The defendants reply that KAYAK's "accuracy checks" do not violate the CFAA. Dkt. No. 378 at 2 n.2, 19 (citing Dkt. No. 343-16, Hemann Decl. Exh. 16 at 222:25- 223:25).

The parties agree that KAYAK accesses the Ryanair website to check the accuracy of flight information provided by its vendors. Accordingly, the resolution of this argument turns on the legal question of whether such access is "without authorization." Because KAYAK accesses only the Ryanair website, which the court finds is public, and not the myRyanair site, the court agrees with the defendants that Ryanair has not produced any evidence that the defendants, including

KAYAK, violate the CFAA through direct access to Ryanair's webpage. The defendants are therefore entitled to summary judgment on the issue of direct liability.

D. Indirect Liability

The parties are in agreement as to many of the central facts underlying this issue. The defendants do not dispute that they received cease-and-desist letters from Ryanair stating that Ryanair did not authorize the OTAs to sell Ryanair flights online. *See* Dkt. No. 335 at 15–16. The parties also agree that the defendants offer Ryanair flights on their platforms, and that the lists of flights are provided to the defendants' third-party vendors. The defendants (other than BHI) also acknowledge that they contract with vendors to populate the defendants' websites with flight information that is ultimately used to book customers' flight itineraries.

In the case of Booking.com, the process of booking a flight is as follows: When a customer searches for a flight itinerary on Booking.com, Booking.com passes the request automatically to its vendor, Etraveli. Etraveli then automatically sends information back to Booking.com listing the flights that meet the customer's search criteria, including any Ryanair flights that may be applicable. The customer then selects a flight and enters the payment details on the Booking.com site. Booking.com then sends the customer's request and payment to Etraveli. Etraveli then books the flight. The customer never leaves Booking.com's website. Declaration of Marcos Guerrero ("Guerrero Decl."), Dkt. No. 337, ¶¶ 5–7. The process is similar for the other defendants and their vendors.

Based on those facts, Ryanair argues that the record conclusively establishes that Booking.com and KAYAK induce, direct, and encourage their vendors—and, for KAYAK only,

commercial partners[14]—to violate the CFAA by sending requests to their vendors to obtain flight information regarding Ryanair flights and to book the flights chosen by their customers. Ryanair argues that those requests can be fulfilled only by circumventing Ryanair's security measures, thereby violating the CFAA. Ryanair also points the court to one of its interrogatory responses in which Ryanair stated that it confirmed that the reservation numbers (referred to as passenger name records or PNRs) provided by the defendants were booked through the Ryanair website. Fuga Decl. Exh. 6 at 83.

The defendants, on the other hand, argue that the facts regarding the process by which information is gathered and flights are booked do not show that any defendant induces, directs, or encourages a third-party vendor to violate the CFAA. First, the defendants argue that the contracts between the defendants and their vendors foreclose indirect liability under the CFAA because those contracts either disclaim an agency relationship explicitly or have terms that specify that the vendor has the discretion to offer and book flights, a process that creates a contract between the customer and the vendor. *See* Hemann Decl. Exh. 49 at 2; Hemann Decl. Exh. 52 § 11.8; Hemann Decl. Exh. 51 at § 14.6, Schedule 2; Hemann Decl. Exh. 54 § 6.1.3; Hemann Decl. Exh. 55 § 6.1(g); Hemann Decl. Exh. 57 §§ 3.6, 10.4; Hemann Decl. Exhs. 56–65. Second, the defendants argue that there is no evidence that the defendants tell their vendors whether to obtain information or to book flights from the Ryanair website, let alone direct their vendors to access the website in a way that violates the CFAA. Third, the defendants argue that there is no evidence that their vendors actually access the Ryanair website.

[14] KAYAK enables both "facilitated bookings," which operate like the other defendants' bookings, and "Link-Out bookings," which are completed entirely on a third-party vendor's page. *See* Fuga Decl. Exh. 4 at 8–11. Thus, for Link-Out bookings, Ryanair argues that KAYAK induces, directs, and encourages its partners, not its vendors.

In their motion to dismiss on the pleadings, the defendants argued that there must be a formal agency relationship between the parties in order to create vicarious liability. In my order on that motion, I rejected that argument and held that the indirect or vicarious liability under section 1030(g) extends to parties who direct, encourage, or induce others to commit acts that violate the CFAA, regardless of whether the parties are in an agency relationship, or whether the defendants' vendors have explicitly agreed to obtain flight information by screen scraping Ryanair's website. *See* Dkt. No. 105 at 7–14. I continue to regard that formulation as stating the proper test for indirect or vicarious liability.

The defendants now argue that indirect liability attaches only if there is "purposeful, active influence by the defendant aimed at the specific computer access at issue—akin to, if not identical to, an agency relationship." Dkt. No. 335 at 19. In support of that standard, the defendants cite *Svanaco, Inc. v. Brand*, 417 F. Supp. 3d 1042 (N.D. Ill. 2019), and *Alchem Inc. v. Cage*, No. 2:20-CV-03142, 2021 WL 4902331 (E.D. Pa. Oct. 21, 2021), *vacated and remanded on other grounds*, 2022 WL 3043153 (3d Cir. Aug. 2, 2022)).

Neither of those cases requires such proof. In *Svanaco*, the court rejected a theory of secondary liability where the defendant's contractor launched a distributed-denial-of-service ("DDoS") attack against the plaintiff, and there was no evidence the contractor informed the defendant that he planned to take such action, let alone that he acted on direction from the defendant. 417 F. Supp. 3d at 1060. In *Alchem*, the court found that the defendant did not direct, encourage, or induce its employee to access the plaintiff's computer system without authorization. 2021 WL 4902331, at *7. The plaintiff in that case argued that the defendant induced one of its employees to violate the CFAA by paying her a commission on sales to new customers, but the

court found it unreasonable to infer that the defendant had induced a violation of the CFAA based solely on the evidence of the employee's pay structure. *Id.*

The defendants' argument that their contracts with their vendors foreclose liability fails under the proper standard for indirect liability. Because indirect liability does not require agency, it is not dispositive that those agreements disclaim an agency relationship: the defendants can be held liable based on evidence that the defendants induced the vendors to violate the CFAA. Additionally, as Ryanair argues in its response to the defendants' motion, it is not relevant under those contracts that a vendor could choose not to display or book Ryanair flights. The defendants' liability does not turn on what the vendors could have done but rather on whether the defendants induced, directed, or encouraged their vendors to obtain flight information from and book flights on Ryanair's website.

Moreover, the defendants are incorrect in asserting that Ryanair can establish liability only if they can show that they specifically directed their vendors to include Ryanair flights and advised them how to access the Ryanair website in a manner that would violate the CFAA, such as by directing their vendors to use bots, to make myRyanair accounts, or to bypass Shield. The defendants' argument on this issue is based on its interpretation of the *Svanaco* and *Alchem* cases. As discussed, however, those cases do not establish that such active direction is required. In those cases, moreover, the defendants never contemplated (let alone directed or encouraged) that third parties would access protected computers. Here, however, even if the defendants were previously unaware of how their vendors were obtaining Ryanair flight information, Ryanair put the defendants on notice of their vendors' conduct through its cease-and-desist letters and stated that Ryanair does not authorize OTAs to sell its flights or scrape its website. *See* Dkt. No. 76, Exhs. B, C, D, & E.

The defendants cannot now avoid liability simply because third parties access the Ryanair website to obtain the relevant information and make bookings for the defendants' customers. *See Power Ventures*, 844 F.3d at 1067 ("Once permission [to access a computer] has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability" under the CFAA.). The evidence is sufficient to create a jury question as to whether the defendants induce, direct, or encourage their vendors to obtain Ryanair flight information and book Ryanair flights by sending requests for these actions from their websites to the vendor websites.[15] The fact that the defendants automated such requests has no bearing on whether there is such direction. If the vendors' actions are in violation of the CFAA, then the defendants can be held liable.

Finally, the defendants' assertion that there is no evidence that their vendors actually access the Ryanair website is incorrect. The parties agree that Ryanair is paid for flights booked on behalf of the defendants' customers by the defendants' vendors. Ryanair points to its interrogatory response stating that Ryanair confirmed that the reservation codes provided by the defendants were purchased through the website, Fuga Decl. Exh. 6 at 83, and argues that any flights booked on the Ryanair website would have to have circumvented Shield. Dkt. No. 348 at 17 (citing Fuga Decl. Exh. 2 at 7-12; Fuga Decl. Exh. 4 at 6-8, 11-14, 17; Fuga Decl. Exh. 19 at 35:12-37:18). The defendants raise issues with Ryanair's interrogatory response, including that it does not explain who at Ryanair made this determination or how that person made the determination. The defendants may raise these issues at trial. For present purposes, Ryanair's summary judgment

[15] Because Ryanair moved for summary judgment only against Booking.com and KAYAK, its motion was directed only to the evidence that those defendants induce, direct, or encourage vendors to access the Ryanair website in violation of the CFAA. Accordingly, Ryanair will need to make the same showing for the other defendants to sustain its charge of indirect liability against them.

motion on this issue is precluded since there is a factual dispute as to whether the defendants' have induced their vendors to access the Ryanair website.

E. The Monex Attack

Monex is Ryanair's payment processor. Whenever a customer tries to make a payment, Ryanair sends Monex a token with the customer's payment information. If the token has no payment information, it is considered a null token. Ryanair keeps an error log of instances in which Monex receives a null token. On October 5, 2023, Ryanair recorded the transmission of more than 60,000 null tokens to Monex in one hour, which adversely affected the functionality of Ryanair's website. *See* Fuga Decl. Exh. 6 at 85–87. Ryanair characterizes that event as the "Monex Attack," and seeks to hold Booking.com liable for that attack.

In their motion for summary judgment, the defendants contend that Booking.com cannot be held liable for the "Monex Attack" for several reasons. Dkt. No. 335 at 22–24. The defendants argue that Booking.com does not access the Ryanair website for customer booking and that any bookings attributable to Booking.com through its vendors could not be responsible for Monex's failure based on the low volume of those bookings during the relevant period. Booking.com also contends that there is no evidence that it directed any of its vendors to launch an attack. Ryanair does not address the "Monex Attack" in its motion for summary judgment.

In response to the defendants' summary judgment motion, Ryanair points to factual disputes that it contends require denial of summary judgment for the defendants on this issue. During discovery, Booking.com produced its PNR codes to Ryanair. Ryanair matched 26 of Booking.com's PNRs from October 5, 2023, to the error log. *See* Fuga Decl. Exh. 6 at 84–86. Ryanair argues that each PNR is likely responsible for thousands of efforts to reach Ryanair's website, which likely contributed to overwhelming Monex. *Id.* at 87. The defendants dispute that

their bookings could have contributed to Monex's failure based on testimony that it is likely that a single source was responsible for the attack. *See* Hemann Decl. Exh. 3 at 79:15–80:14. The defendants also point to statements that a third party could have been entirely responsible for the incident. *See id.* at 63:14-64:3, 79:23-80:24. In addition, the defendants argue that in the case of the specific PNR code connected to 5000 payments attempts, it was the computer's IP address that was associated with those attempts, but not the specific session connected with Booking.com's PNR code. *See* Dkt. No. 378 at 5–6 n.6. Ryanair will need to prove at trial that the attempts associated with Booking.com could be responsible for all or part of the breakdown of its website functionality, but that issue cannot be resolved at this juncture.

The defendants' first argument—that Booking.com does not directly access the Ryanair website—is beside the point, because both parties agree that access to the website happens through third parties. As noted above, in order for any liability to attach to Booking.com, Ryanair must prove that Booking.com is vicariously liable for violations of the CFAA.

The defendants' second argument—that Booking.com was unaware of the attack and thus could not have directed, induced, or encouraged it—is similarly unavailing. The defendants compare this case to *Svanaco*, in which the defendant did not know its contractor was launching an attack on the plaintiff's website and was therefore held not to be liable for the consequences of the attack. 417 F. Supp. 3d at 1060. The defendants point in particular to evidence that Booking.com did not know why its vendors had issues accessing the Ryanair website on October 5 and 6, 2023, and they contend there is no evidence that Booking.com directed the attack or intended to cause the outage. *See* Hemann Decl. Exh. 13 at 22:8–24:15; Guerrero Decl. [Dkt. No. 337] ¶¶ 13–14; Housseau Decl. [Dkt. No. 338] ¶¶ 4–6 and Exh. A.

Ryanair's theory, however, is not that Booking.com specifically directed its vendors to act so as to overwhelm Monex, but rather that Booking.com is liable because it directed, induced, or encouraged accessing the website in violation of the CFAA by sending customer requests to third-party vendors who necessarily had to overcome Ryanair's security measures. Accordingly, even if Booking.com did not direct its vendors on how to overcome those measures, such as by disabling Shield by submitting multiple payment attempts to Monex, Booking.com could be held liable for inducing, directing, or encouraging such action if the defendants had the intent to induce their vendors to obtain information from the Ryanair website by circumventing Ryanair's attempts to prevent them from doing so.

F. Count I: 18 U.S.C. § 1030(a)(2)(C)

A defendant violates Section 1030(a)(2)(C) when it accesses a computer intentionally without authority or exceeding authorized access and thereby obtains information from a protected computer. As noted earlier, all the information that is obtained from the Ryanair website by screen scraping is obtained from the public portion of the website, not from the password-protected payment page of myRyanair. Therefore, the defendants do not obtain information by accessing a computer without authorization or by exceeding their authorized access. For that reason, summary judgment must be granted to the defendants with regard to Count I of the complaint.

G. Count IV: 18 U.S.C. § 1030(a)(5)(B)–(C).

Ryanair argues for summary judgment against Booking.com and KAYAK under sections 1030(a)(5)(B) and (C) of the CFAA, which prohibit knowingly causing a transmission that intentionally accesses a protected computer without authorization and either recklessly causes damage (subparagraph (B)) or causes damage and loss (subparagraph (C)). Ryanair argues that it has suffered damage based on the "Monex Attack" as well as other injury to its data integrity. The

defendants argue that Ryanair's damages claim fails because no evidence links any defendant to the Monex attack and because adding passenger data does not denigrate data integrity as contemplated under the CFAA but rather is simply data that Ryanair does not find optimal from a business standpoint. For the reasons discussed in sections II.B.ii and II.G, issues of fact preclude summary judgment on this count.

H. Count II: Fraud under 18 U.S.C. § 1030(a)4).

The defendants have moved for summary judgment on Ryanair's fraud claim under section 1030(a)(4), contending that there is no evidence the defendants knowingly accessed the Ryanair's website with the intent to defraud Ryanair. Their argument about knowing access revisits their arguments about vicarious liability addressed above, and will not be addressed again here. The defendants also argue there is no evidence of intent to defraud because there is no proof that the defendants had the intent to "deceive or to cheat," *see Fidlar Techs. V. LPS Real Estate Data Sols., Inc.*, 810 F.3d 1075, 1079 (7th Cir. 2016), or that the defendants "contemplated some actual harm or injury to their victims," *see United States v. Starr,* 816 F.2d 94, 98 (2d Cir. 1987). The defendants point to the legislative history of the CFAA to support their contention that proof of an "intent to defraud" for purpose of the CFAA must meet an exacting standard. *See United States v. Czubinski*, 106 F.3d 1069, 1078-79 (1st Cir. 1997) (citing S. Rep. No. 432, 99th Cong., 2d Sess., reprinted in 1986 U.S.C.C.A.N. 2479, 2488) (the CFAA's legislative history distinguishes "between computer theft . . . and computer trespass" and that requiring a showing of an intent to defraud for purposes of section 1030(a)(4), "is meant to preserve that distinction").

Ryanair argues that this court should not apply that restrictive standard for fraud under the CFAA. Rather, according to Ryanair, the court should follow the definition of fraud set forth in *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1126 (W.D.

Wash. 2000), which was adopted by a district court in this circuit. *See Volpe v. Abacus Software Sys. Corp.,* No. CV2010108*,* 2021 WL 2451968, at *5 (D.N.J. June 16, 2021); *see also Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc.*, 556 F. Supp. 2d 1122, 1131 (E.D. Cal. 2008). The *Shurgard* court held that under the CFAA, "fraud simply means wrongdoing and not proof of the common law elements of fraud." 119 F. Supp. 2d at 1126. Under that standard, Ryanair argues, there is evidence that the defendants acted with the intent to defraud by working with their vendors to facilitate unauthorized access to the Ryanair website. In any event, Ryanair argues that even under the stricter standard, it has shown that the defendants engaged in fraud because they knew their actions were harming Ryanair but continued their course of action nonetheless.

Although the parties focus their briefing on a dispute over the meaning of the phrase "intent to defraud," the cases the parties cite are largely in agreement regarding the proper standard. In *Fidlar Technologies*, the Seventh Circuit held that the phrase "intent to defraud" in the CFAA requires a specific intent to "deceive or cheat, usually for the purpose of getting financial gain for himself or causing financial loss to another." 810 F.3d at 1079.[16] In *Shurgard*, the court held that fraud requires the defendant employ "dishonest methods" to carry out a violation of the CFAA. 119 F. Supp. 2d at 1125–26. Courts applying *Shurgard* look for evidence of deceit. *See, e.g., Volpe*, 2021 WL 2451968, at *4–5 (plaintiff sufficiently pleaded fraud under the CFAA by alleging that the defendant deceived Apple Inc. into believing the plaintiff, rather than the defendant, was accessing the plaintiff's account); *SMH Enterprises, L.L.C. v. Krispy Krunchy Foods, L.L.C*, No.

[16] The defendants appear to focus on the latter half of the pertinent sentence in the *Fidlar* case to support their argument that they have not caused financial loss to Ryanair because Ryanair is paid for its flights. However, in the present case, Ryanair argues that the defendants gain something of value through selling Ryanair flights, which invokes the first half of the pertinent sentence in *Fidlar*.

CV 20-2970, 2021 WL 1226411, at *5–6 (E.D. La. Apr. 1, 2021) (explaining that the *Shurgard* definition "usually signifies the deprivation of something of value by trick, deceit, chicane, or overreaching") (citation omitted).

Because section 1030(a)(4) itself requires the defendant to have obtained something of value, the element of financial gain is often discussed separately from the element of "intent to defraud." However, the *Czubinski* court, which both sides cite to as supporting their respective proposed standards, explained that the requirement in section 1030(a)(4) that the defendant obtain something of value operates like the requirement that there be a deprivation of property for federal mail fraud violations. *See* 106 F.3d at 1079. The court explained that to constitute deprivation, "some articulable harm must befall the holder of the information as a result of the defendant's activities, or some gainful use must be intended by the person accessing the information, whether or not this use is profitable in the economic sense." *Id.* at 1074. That characterization is entirely consistent with standard articulated by the court in *Fidlar Technologies*.

A genuine issue of material fact precludes summary judgment on this claim. Ryanair has produced evidence that the defendants access the Ryanair website by dishonest means, that is, by using "false" contact and payment information. Whether or not Ryanair ultimately receives payment for the flights booked through the defendant OTAs, Ryanair may still be able to show that the defendants have acted act with the intent to deceive Ryanair by using false information to obtain something of value: to wit, profitable flight bookings that the defendants would not be able to obtain otherwise.

I. Count V: Conspiracy under 18 U.S.C. § 1030(b).

The defendants argue that there is no evidence to sustain Ryanair's conspiracy claim under 18 U.S.C. § 1030(b), because the defendants' vendor contracts do not establish a CFAA

conspiracy. The defendants argue that because the contracts do not reference Ryanair at all, let alone constitute an agreement about how to access Ryanair's website in violation of the CFAA, Ryanair cannot show that the defendants had the specific intent to "further the substantive offense" under the CFAA. *See United States v. Carbo*, 572 F.3d 112, 116 n.2 (3d Cir. 2009). The defendants further argue, as they did regarding indirect liability, that they lack control over which airlines and flights their vendors source and how their vendors source those flights. Regarding BHI and Agoda specifically, the defendants argue there is no agreement with any vendor to source Ryanair flights at all.

Ryanair responds that there is sufficient evidence of conspiracy to justify submitting that issue to the jury at trial. Ryanair contends that a conspiracy claim under the CFAA requires "evidence of an agreement and common activities in furtherance of the unlawful act," *see Welenco Inc. v. Corbell*, 126 F. Supp. 3d 1154, 1176 (E.D. Cal. 2015), and that the defendants' websites and vendor agreements provide that evidence. Ryanair's theory of conspiracy is similar to its theory of indirect liability—that the defendants pass specific requests for flight information and flight bookings to their vendors via Application Programming Interface ("API") connections.[17] This, Ryanair argues, is evidence that the defendants have agreed to violate the CFAA. With regard to Agoda, Ryanair argues that Agoda procures its bookings through Priceline and Priceline's vendors. Ryanair also argues that the agreements between the defendants and their vendors (or, for Agoda, an agreement between two defendants) constitute evidence of agreement to engage in conduct that violates the CFAA. Moreover, Ryanair argues that because the defendants can control what airlines are displayed on their websites, the defendants necessarily

[17] An API connection allows two systems to exchange data. API connections may integrate two or more applications running on the same website or, as the case is here, applications running across different websites.

make a conscious decision to include Ryanair flights and thus to participate in the conspiracy to violate the CFAA as it relates to those flights.

I addressed the conspiracy claim at the motion to dismiss phase and found that Ryanair had plausibly alleged a claim under section 1030(b) on the ground that the defendants had entered into agreements with vendors to access the Ryanair website without authorization, despite knowing that neither the defendants nor their agents had authorization to do so. *See* Dkt. No. 105 at 25–27; *see also In re Lenovo Adware Litig.*, No. 15-MD-02624, 2016 WL 6277245, at *6 (N.D. Cal. Oct. 27, 2016) (A claim under section 1030(b) requires "specific allegations of an agreement and common activities").

Ryanair has now produced sufficient evidence to support those allegations so that summary judgment on the conspiracy claim would be inappropriate. The defendants have produced contracts with their vendors, as discussed above, demonstrating an agreement to book flights on behalf of the defendants. Pursuant to those agreements, the defendants send requests to their vendors, which are automated via API connection, to purchase Ryanair flights. Ryanair argues that those purchases require circumventing the myRyanair password gate, which could qualify as unlawful conduct under the CFAA. Ryanair also points to evidence that the defendants knew or should have known that its vendors were accessing protected portions of the Ryanair website without authorization, evidence that includes the allegations in the complaint, allegations made in Ryanair's cease-and-desist letters, and, in the case of Booking.com, an inquiry into its vendors' screen-scraping practices. *See* Fuga Decl. Exhs. 24 & 25.

Ryanair responds to the defendants' contentions that they do not control which airlines' flights are displayed on their websites. Ryanair cites testimony from the defendants' witnesses that they can stop displaying Ryanair flights. *See* Mao Decl. Exh. 9 at 191:12–193:1 (testimony

on how Agoda blocks Ryanair flights); Mao Decl. Exh. 10 at 30:15–22 (testimony that Priceline can turn off specific airlines); Hemann Decl. Exh. 12 at 25:1–26:14 (testimony that Booking.com can instruct Etraveli to remove certain airlines from the flight information it shares with Booking.com).

Contingent on Ryanair's ability to prove the alleged unlawful access, a reasonable juror could find a knowing "agreement and common activities in furtherance of the unlawful act." *See Welenco*, 126 F. Supp. 3d at 1176 (citing *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816 (N.D. Cal. 2014); *Vacation Club Servs., Inc. v. Rodriguez,* No. 6:10–cv–247, 2010 WL 1645129, at *1–2, (M.D. Fla. Apr. 22, 2010); *see also United States v. Koshkin*, No. 21-3085, 2024 WL 1927855 (2d Cir. May 2, 2024) (holding that there was "sufficient evidence from which a jury could reasonably" find a conspiracy to commit a violation of the CFAA where the government presented evidence that the defendant knew his coconspirator was operating an illegal botnet and the defendant provided crypting services for his coconspirator).[18]

Regarding Agoda, the defendants argue for summary judgment on the ground that Agoda does not have agreements with vendor. However, Agoda has an agreement with Priceline, under which Agoda facilitates bookings of Ryanair flights for its customers via an API connection with either Priceline or Priceline's vendors. *See* Hemann Decl. Exh. 34 at 9. That is enough to avoid summary judgment on the conspiracy count as applied to Agoda.

Regarding BHI, Ryanair does not dispute that BHI is not party to any vendor agreement—which is unsurprising given that BHI is a holding company—nor did it advance any other basis in

[18] A botnet is a group of computers that can be used for criminal activity, including infecting other computers with malware and launching DDoS attacks. Crypting is a service that modifies malware so that it cannot be detected by antivirus programs.

its briefing for finding BHI liable for conspiracy in for BHI.[19] Because this issue was not addressed in the parties' briefs, I will postpone any ruling on the issue until trial. Accordingly, for present purposes, summary judgment is denied as to each of the defendants on Count V.

J. Ryanair's Request for a Permanent Injunction

The defendants seek summary judgment against Ryanair on its request for a permanent injunction on the ground that Ryanair has not shown that it is faced with irreparable harm and has not shown that it lacks an adequate remedy at law. *See* Dkt. No. 335 at 37–38 (citing *TD Bank N.A. v. Hill*, 928 F.3d 259, 278 (3d Cir. 2019). Because Ryanair does not dispute that it is paid for the tickets that the defendants purchase from Ryanair on behalf of their customers, the defendants argue Ryanair cannot show that it is faced with any irreparable harm.

The question whether an injunction (or any other form of relief) should be granted is premature at this juncture. Entitlement to either legal or equitable relief can be decided by the court in the event that there is a finding of liability on any of Ryanair's CFAA claims.

IV. Ryanair's Motion for Summary Judgment on Booking.com's State Law Counterclaims

Booking.com has asserted five state law counterclaims against Ryanair: (1) tortious interference with business relations, (2) unfair competition, (3) trade libel, (4) defamation based on Ryanair's statements to customers,[20] and (5) deceptive trade practices. Ryanair argues that for

[19] During the argument on the motions for summary judgment, Ryanair suggested that BHI could be held liable for conspiring with its wholly owned subsidiary, Booking.com. That proposition is questionable in light of the principle that, at least in the antitrust context, a corporation cannot conspire with its wholly owned subsidiary. *See Copperweld Corp. v. Independence Tube Corp.*, 467 U.S. 752 (1984). The parties should be prepared to address this issue at trial in the event that Ryanair seeks to press its claim of conspiracy against BHI.

[20] In my order on Ryanair's motion to dismiss, I dismissed those portions of Booking.com's defamation counterclaim that were based on Ryanair's public statements but denied the motion to dismiss as it related to those portions of Booking.com's defamation counterclaim that were based on Ryanair's statements to customers. Dkt. No. 134 at 11–17.

three reasons summary judgment should be granted in its favor on some or all of the five counterclaims. First, Ryanair argues that Booking.com's counterclaims for defamation, trade libel, and deceptive trade practices must fail because Ryanair's statements underlying those counterclaims are true. Second, Ryanair argues that Booking.com cannot prove that Ryanair acted wrongfully and thus cannot prevail on its tortious interference and unfair competition claims. Third, Ryanair argues that Booking.com cannot prove damages, a required element of tortious interference, unfair competition, and trade libel. In its response, Booking.com argues that material issues of genuine fact foreclose summary judgment as to any of the defendants' counterclaims.

A. Falsity: Booking.com's defamation, trade libel, and DTPA claims

In its brief in opposition to Ryanair's motion for summary judgment, Booking.com points to three Ryanair statements that form the bases for Booking.com's counterclaims of defamation, trade libel, and violations of Delaware's Deceptive Trade Practice Act ("DTPA"), 6 Del C. § 2531 *et seq*.[21] Those statements are:

> 1. "Unauthorized OTAs . . . use 'screen scraper' software to mis-sell Ryanair flights in breach of the Terms of Use of the Ryanair website."
>
> 2. "Screen scraper OTAs provide Ryanair with false customer details which prevents us from notifying passengers" and the "false payment and contact details screen scraper OTAs provide Ryanair for customers inhibits Ryanair from providing our post-contractual obligations."
>
> 3. "Screen scraper OTAs provide Ryanair with false customer details which prevents us from notifying passengers of important safety, security and public health requirements."

Dkt. No. 372 at 30, 33, 34. Booking.com argues that there is a genuine issue of material fact as to the truth of each of those statements.

[21] The parties agree that the tort claims set forth in Booking.com's counterclaims are governed by Delaware law.

i. Burden of Proof

The parties disagree about which party has the burden of proof with respect to the issue of falsity. In a defamation case, when statements are directed to a matter of public concern, the plaintiff bears the burden of proving the statements are false.[22] *See Cousins v. Goodier*, 283 A.3d 1140, 1148 n.40 (Del. 2022). Ryanair argues that its emails addressed a matter of public concern because "they communicate steps customers must take so that Ryanair can notify them of important safety, security and public health requirements, and they inform customers about the effects of booking with unauthorized OTAs." *See* Dkt. No. 348 at 27 n.14 (quotations omitted). Booking.com argues that the emails were merely part of Ryanair's effort to encourage customers to use Ryanair's website instead of using an OTA to book flights. For that reason, Booking.com argues, the emails do not address a matter of public concern, and therefore Ryanair, not Booking.com, has the burden of proof on the issue of falsity. *See* Dkt. No. 372 at 30 n.12.

"Speech deals with matters of public concern when it can 'be fairly considered as relating to any matter of political, social, or other concern to the community,' or when it 'is a subject of legitimate news interest; that is, a subject of general interest and of value and concern to the public.'" *Snyder v. Phelps*, 562 U.S. 443, 453 (2011) (citations omitted). "To determine whether speech is of public or private concern, [the court] must independently examine the 'content, form, and context' of that speech" in light of the whole record. *Id.*

[22] Falsehood is an element of Booking.com's trade libel and deceptive practices claim, and Booking.com therefore has the burden of proof to show that Ryanair's statements were false. *See In re Nat'l Collegiate Student Loan Trs. Litig.*, No. CV 12111, 2020 WL 3960334, at *4 (Del. Ch. July 13, 2020) (explaining that "trade libel" is "predicated on 'the knowing publication of false material that *is derogatory* to the plaintiff's business.'"); 6 Del. C. § 2532(a)(8) (defining one deceptive practice as "[d]isparag[ing] the goods, services, or business of another by false or misleading representation of fact"); *see also* Dkt. No. 111 at 72–73 (alleging a deceptive trade practice claim based on Ryanair's assertedly false or misleading statements).

Ryanair's emails to passengers who booked flights through OTAs address a matter of private concern. While safety, security, and public health requirements are often matters of public concern, the content, form, and context of Ryanair's emails make clear that Ryanair was addressing a matter of private concern. The content of the speech did not directly address issues of safety, security, and public health, but rather informed customers who booked Ryanair flights through an OTA that Ryanair may not have their correct contact information, which could prevent Ryanair from disseminating information to them about "safety, security, and public health protocols." *See* Dkt. No. 111 at 60–61. Essentially, the email addressed Ryanair's business practice regarding the dissemination of relevant information to its customers by email.

The form and context of the Ryanair emails also indicate that the subject of the emails was a matter of private concern. While not dispositive, *see Cousins*, 283 A.3d at 1152, Ryanair's use of private emails sent to a subset of its customers on a specific subject pertinent to those customers supports the conclusion that the emails addressed a matter of private concern. *Compare Synder*, 562 U.S. at 454–55 (protest on public land next to a public street was of public concern), *and Cousins*, 283 A.3d at 1152 (an email relating to a local political issue that was widely shared on Facebook with members of the plaintiff's professional and geographic community was a matter of public concern), *with Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 762 (1985) (an individual's credit report shared by a business with a limited number of subscribers was a matter of private concern). Because the Ryanair emails do not address a matter of public concern, Ryanair bears the burden of proof on the issue of falsity.

ii. Statement 1: "Unauthorized OTAs . . . use 'screen scraper' software to mis-sell Ryanair flights in breach of the Terms of Use of the Ryanair website."

Ryanair argues that Statement 1 is true in its entirety. First, Ryanair contends that it is accurate to say that the OTAs use "screen scraper" software because Booking.com sells its flights

exclusively through Etraveli, and Booking.com is aware that Etraveli uses screen scraping. *See* Fuga Decl. Exh. 3 at 40:5–8, 43:9–16; Fuga Decl. Exh. 24 at BOOKING.COM00002386; Fuga Decl. Exh. 25. Second, Ryanair argues that in this context the term "mis-sell" means to sell flights without authorization and in violation of Ryanair's terms of use. In support, Ryanair cites my order on Ryanair's motion to dismiss the counterclaims, in which I stated that "the assertion that Booking.com is 'unauthorized' is true, as it is undisputed that Ryanair has not authorized Booking.com to sell tickets for Ryanair flights." Dkt. No. 134 at 13.

In its response, Booking.com argues (1) that the evidence clearly shows that Booking.com itself does not access Ryanair's website, nor has it agreed to Ryanair's terms of use such that Booking.com has breached any obligation to Ryanair; (2) that Booking.com does not "mis-sell" Ryanair flights, as mis-selling refers to the act of misleading customers in order to make a sale; and (3) that Booking.com does not "mis-sell" Ryanair flights by selling tickets contrary to Ryanair's terms of use, because Booking.com does not go onto the Ryanair website.

There is a genuine dispute as to the truth of the first half of Statement 1. Whether Etraveli uses screen scraping is contested. Ryanair's own evidence is not conclusive on this issue: It shows that Booking.com asked Etraveli about screen scraping, *see* Fuga Decl. Exh. 24, and that Booking.com received a response that explained how Etraveli uses a screen-scraping process, *see* Fuga Decl. Exh. 25. However, Etraveli's response makes clear that Etraveli does not always use screen scraping, and it does not confirm what process Etraveli uses on the Ryanair website specifically. *See* Fuga Decl. Exh. 25. Booking.com disputes that Ryanair can show that any of the defendants' vendors, including Etraveli, access the Ryanair website by the use of screen-scraping bots, *see supra* section III.D.

There is, however, no dispute as to the truth of the second half of the sentence. Ryanair argues that the sentence, read in full, defines mis-selling flights by reference to the Ryanair website's terms of use ("OTAs . . . mis-sell Ryanair flights in breach of the Terms of Use of the Ryanair website.") *See* Dkt. No. 111 at 61. Booking.com argues that Ryanair itself is not consistent as to what "mis-selling flights" means, as Ryanair's CEO used the term "mis-sell" to refer to inflating the costs of Ryanair flights and selling outside of the Ryanair website. *See* Declaration of Kathleen Hartnett ("Hartnett Decl."), Dkt. No. 374, Exh. D at 8:8–12, 20:8–18. In addition, Booking.com points out that the term "mis-sell" refers to a crime in the United Kingdom (perhaps forgetting for the moment that the Republic of Ireland is decidedly not a part of the U.K.).[23]

In the context of the statement at issue, however, it is evident that the use of the term "mis-sell" is cabined by the phrase "in breach of the Terms of Use of the Ryanair website." No reasonable reader would assume that the term "mis-sell" in Statement 1 refers to a criminal act, even if the term "mis-sell" standing alone would be open to multiple meanings.[24]

Booking.com also focuses heavily on the undisputed fact that Booking.com itself does not access Ryanair's website. However, Ryanair is correct that its statement is still "substantially true" if Etraveli, rather than Booking.com, scrapes the Ryanair website and does so at Booking.com's behest. *See Riley v. Moyed*, 529 A.2d 248, 253 (Del. 1987) ("[T]here is no liability for defamation

[23] *See Financial services mis-selling: regulation and redress*, National Audit Office (Feb. 24, 2016), https://www.nao.org.uk/reports/financial-services-mis-selling-regulation-and-redress (defining mis-selling as "providing customers with misleading information or recommending that they purchase unsuitable products").

[24] Ryanair argues in its reply brief that the "innocent construction rule" applies here. *See* Dkt. No. 380 at 12 (arguing that a statement that can reasonably be given an innocent interpretation is not actionable). However, the "innocent construction rule" is a minority rule not followed by Delaware. *See* Rodney A. Smolla, LAW OF DEFAMATION § 4:21 (2d ed. 2024).

when a statement is determined to be substantially true.") Under Delaware law, "[i]f the alleged libel was no more damaging to the plaintiff's reputation in the mind of the average reader than a truthful statement would have been, then the statement is substantially true." *Id*. In this case, it would be no more damaging to say Booking.com uses third party vendors to screen scrape the Ryanair website than to say that Booking.com does the screen scraping itself. Accordingly, Booking.com's argument that it does not itself access the Ryanair website to screen-scrape the website in violation of Ryanair's terms of use does not negate the truth of Ryanair's statement if Ryanair can prove that Booking.com's vendors take that action at the behest of Booking.com.

iii. Statement 2: "Screen scraper OTAs provide Ryanair with false customer details which prevents us from notifying passengers" and "false payment and contact details screen scraper OTAs provide Ryanair for customers inhibits Ryanair from providing our post-contractual obligations."

This statement is part of an email that Ryanair is alleged to have sent to customers who appeared to Ryanair to have purchased tickets through an OTA. The email in question added that the false customer details prevented Ryanair from notifying passengers "of important safety, security, and public health requirements." Dkt. No. 111 at 60. Ryanair argues that there is no genuine issue of material fact as to the truth of its statements that OTAs provide "false" customer information because (1) Booking.com admitted it does not share customer credit card information with Etraveli; (2) Booking.com is not aware of whether Etraveli provides the customer's correct email address to Ryanair, and (3) according to Ryanair expert Iain Lopata, Booking.com uses disposable email addresses and virtual credit card numbers to create myRyanair accounts. *See* Fuga Decl. Exh. 3 at 87:18–88:8, 102:3–20; Lopata Decl. ¶¶ 10(d), 20–37.

Booking.com argues that there is a genuine dispute regarding the truth of this statement for three reasons. First, Booking.com again argues that it does not directly access the Ryanair

website.[25] Second, Booking.com argues that the term "false" in the statement suggests that the customer's information in question is "illegitimate" or "fraudulent" rather than simply not the passenger's actual contact information, since there is no dispute that Ryanair gets paid for the OTA bookings. *See* Hemann Decl. Exh. 7 at 30:20–23; Hemann Decl. Exh. 6 at 175:25–176:4. Third, Booking.com argues that the evidence shows that Ryanair receives the passenger's own contact information for bookings. *See* Lopata Decl. ¶ 34(n); Hemann Decl. Exh. 41 at 78–86; Hartnett Decl. Exh. L at 15, Row 2 (customer email was correct); Hartnett Ex. N at 1 of 10, Row 3 (customer's "own email and credit card"), 3 of 10, Row 2 ("email correct"); 8 of 10, Row 18 ("mail ok").

There is a genuine dispute as to the truth of Ryanair's statement. First, the parties dispute whether a reader of the email would interpret the email to mean that Booking.com provided information other than the customers' information or whether Booking.com provided fraudulent information. Ryanair argues that, in context, the reference to "false" details means "incorrect" details, because Ryanair states that receiving such "false" information prevents Ryanair from "notifying passengers" and "providing its post-contractual obligations." *See* Dkt. No. 111 at 60. Booking.com argues that the term "false" implies that Booking.com engaged in fraudulent payment methods. Here, it is not clear in context whether Ryanair's alleged inability to notify customers and satisfy its contractual obligations is due to its receipt of incorrect or fraudulent information. Because the email is open to multiple meanings, "it is for 'the trier of fact [to] determine whether the language used was actually understood in its defamatory sense.'" *See*

[25] For the reasons addressed in the discussion of Statement 1, if it is true that Etraveli provides Ryanair with "false" payment information and customer emails at Booking.com's behest, then Ryanair's statement would still be substantially true because Booking.com makes its bookings through Etraveli.

Bobcat N. Am., LLC v. Inland Waste Holdings, LLC, No. N17C-06-170, 2019 WL 1877400, at *17 (Del. Super. Ct. Apr. 26, 2019) (quoting *NITV, L.L.C. v. Baker*, 61 So. 3d 1249, 1252 (Fla. Dist. Ct. App. 2011)).[26]

Second, there is a genuine dispute as to whether Booking.com provides incorrect customer information to Ryanair. Regarding customer payment information, Ryanair's own evidence is not conclusive. The cited deposition testimony states that under one model, Booking.com provides the customer's credit card information to Etraveli, but under a second model, it does not. Fuga Decl. Exh. 3 at 87:18–88:8. Booking.com points to evidence that at least one Ryanair booking made through Booking.com is associated with the passenger's "own email and credit card." Declaration of Kathleen Hartnett ("Hartnett Decl."), Dkt. No. 374, Exh. N. at RYANAIR-BOOKING_0040319 1 of 10, row 3. Ryanair relies on its expert's testimony to support its contention that Ryanair does not receive the correct customer email addresses from purchases made through Booking.com, *see* Lopata Decl. ¶¶ 20–37. Booking.com, however, responds that in most cases "the Defendants provided the correct customer email address to Ryanair, even though it was not used to create the myRyanair account." *Id.* at ¶ 34(n); *see* Hartnett Decl. Exh. L at 15 of 24, row 2 ("Email was correct" for a Ryanair booking); Hartnett Decl. Exh. M at 2. In short, there is a factual dispute as to whether Ryanair's statement is true or substantially true.

[26] While the Superior Court of Delaware in the *Bobcat* case was applying Florida law, the elements of defamation under Florida law are the same as the elements of defamation under Delaware law. *Compare id.* ("Florida law provides, [t]o establish a cause of action for defamation, a plaintiff must show that (1) the defendant published a false statement about the plaintiff, (2) to a third party, and (3) the falsity of the statement caused injury to the plaintiff") (internal quotation marks omitted), *with Grubbs v. Univ. of Del. Police Dep't*, 174 F. Supp. 3d 839, 861 (D. Del. 2016) ("To state a cause of action for defamation under Delaware law, a plaintiff must plead . . . (1) the defamatory character of the communication; (2) publication; (3) that the communication refers to the plaintiff; (4) a third party's understanding of the communication's defamatory character; and (5) injury.").

iv. Statement 3: "Screen scraper OTAs provide Ryanair with false customer details which prevents us from notifying passengers of important safety, security and public health requirements."

Booking.com's Statement 3 substantially overlaps with Statement 2, adding only the portion of the statement asserting that the false customer details provided by the OTAs prevent Ryanair from notifying its passengers "of important safety, security and public health requirements." In its counterclaims, Booking.com characterized Ryanair's third statement as an assertion that "OTAs, including Booking.com, fail to 'confirm compliance with required safety, security and public health protocols' or 'requirements.'" *See* Dkt. No. 111 at 71. From both sides' briefing, however, it is apparent that the latter statement does not appear in any of the Ryanair emails that Booking.com has pointed to as actionable. Statement 3, as Booking.com has now framed it, cannot be treated as a separate defamatory statement.

v. Actual Malice

Ryanair argues that Booking.com cannot prove its trade libel claim or request punitive damages for its defamation claim, because both require Booking.com to prove that Ryanair acted with actual malice. Ryanair asserts that Booking.com has not made such a showing because the evidence shows that Ryanair did not make the challenged statements with knowledge of their falsity or with reckless disregard for their truth or falsity. Dkt. No. 348 at 31.

Booking.com argues that Ryanair has not shown that the "actual malice" standard applies to this case. Even if it does, Booking.com argues, there is evidence that Ryanair acted with actual malice because Ryanair's internal records show (1) that Booking.com provided Ryanair with correct customer email addresses and (2) that Ryanair knew it did. Additionally, Booking.com argues that the actual malice standard does not apply to its defamation claim because Ryanair's speech constitutes commercial speech to which the actual malice standard does not apply. Dkt. No. 372 at 35–36.

As Ryanair points out, I have already addressed this issue and have held that a claim for trade libel requires a plaintiff to show that the defendant acted with actual malice. *See* D.I. 134 at 17 (citing *Nat'l Collegiate Student Loan Trs. Litig.*, 2020 WL 3960334, at *4; Restatement (Second) of Torts § 623A cmts. d, g.). Thus, Booking.com is incorrect in asserting that Ryanair has failed to show that the "actual malice" standard applies in this case.[27] In addition, a plaintiff ordinarily must show actual malice to be awarded punitive damages. *See Cousins*, 283 A.3d at 1149 n.42. However, if Booking.com is correct that Ryanair's emails are properly characterized as commercial speech, then the heightened standard of actual malice does not apply to Booking.com's defamation claim. *See U.S. Healthcare, Inc. v. Blue Cross of Greater Philadelphia*, 898 F.2d 914, 937 (3d Cir. 1990).

For purposes of Booking.com's trade libel claim, there is a genuine factual dispute as to whether Ryanair made its statements that OTAs have provided Ryanair with false customer information, knowing that the statements were false or, alternatively, whether Ryanair made those statements in reckless disregard of their truth or falsity. As discussed previously, there is a genuine dispute as to whether Ryanair receives incorrect information from bookings made by OTAs. Booking.com relies on Ryanair's own records to show that Ryanair often received correct

[27] To the extent Booking.com is referring to Ryanair's argument at the motion to dismiss stage that actual malice applies to Booking.com's defamation claims because Booking.com is a public figure, Booking.com is correct that Ryanair has not substantiated that claim for purposes of summary judgment. In its opening summary judgment brief, Ryanair argued that Booking.com must show actual malice as it relates to Booking.com's trade libel claim and punitive damages for defamation. *See* Dkt. No. 348 at 31. In its reply brief, Ryanair additionally argued that Booking.com is a limited purpose public figure but its only analysis on that argument appeared in a parenthetical stating "Booking is a public figure because its use of the Ryanair logo suggests to the public that it has authorization to sell Ryanair flights." *See* Dkt. No. 380 at 15. That argument falls far short of showing that Booking.com has thrust itself into a public controversy and thus "effectively assumed the risk of potentially unfair criticism." *See Computer Aid, Inc. v. Hewlett-Packard Co.*, 56 F. Supp. 2d 526, 536–537 (E.D. Pa. 1999).

customer email addresses, even if the customer's myRyanair account was initially opened with a temporary email address that was not the customer's real email address. *See, e.g.,* Lopata Decl. ¶ 34(n); Hemann Decl. Exh. 41 at 73–86. At trial, Booking.com will need to demonstrate that such knowledge is attributable to "the individuals actually involved in approving the publication" of the accused statement, not merely to Ryanair as an institution. *Page v. Oath Inc.*, 270 A.3d 833, 850 (Del. 2022). For present purposes, however, Booking.com has produced sufficient evidence to show that there is a genuine factual dispute on that issue and thus to avoid summary judgment.

Regarding Ryanair's statement that the OTAs use screen-scraper software to mis-sell flights, Booking.com relies heavily on its understanding of the term "mis-sell." *See* Dkt. No. 372 at 35–36. Having already determined that "mis-sell" is best understood to refer to violations of the Ryanair website's terms of use, there is no evidence that Ryanair made that statement with knowledge that the statement was false or was made in reckless disregard of its truth or falsity. In fact, there is no dispute that OTAs violate the terms of use of Ryanair's website, which explicitly state that Ryanair's website is the only website authorized to sell Ryanair flights and explicitly prohibit screen scraping. Dkt. No. 76-1. Regarding the first half of the subject statement— that "Unauthorized OTAs . . . use 'screen scraper' software"—there is also no evidence that Ryanair acted with actual malice. Even if Ryanair cannot show that, as applied to Booking.com, Booking.com's vendor did not use screen scraping software, there is nothing to suggest that Ryanair knew that statement was false or acted with reckless disregard to its truth as it relates to OTAs generally.

For purposes of Booking.com's defamation claim, there is a genuine factual dispute as to whether Ryanair's statements are properly characterized as commercial speech, and thus whether the actual malice standard applies. In determining whether speech is commercial, courts consider factors such as whether the speech is an advertisement, whether the speech refers to a specific product

or service, and whether the speaker had an economic motivation for making the statements in question. *U.S. Healthcare*, 898 F.2d at 933. Neither party has developed this argument at this stage, but it is evident that the parties continue to dispute whether Ryanair's speech was economically motivated. Booking.com argues that Ryanair's emails are part of its anti-OTA business strategy, whereas Ryanair argues that its emails are motivated by its need to comply with relevant regulations.[28]

B. Booking.com's Tortious Interference and Unfair Competition Claims

The elements of tortious interference with prospective business relations under Delaware law are (1) a reasonable probability of a business opportunity; (2) intentional interference by the defendant with that opportunity; (3) proximate causation; and (4) damages. *Empire Fin. Servs., Inc. v. Bank of N.Y. (Del.)*, 900 A.2d 92, 98 n.19 (Del. 2006) (citation omitted); *see also Mondero v. Lewes Surgical & Med. Assocs., P.A.*, No. 14-588, 2018 WL 1532429, at *4 (D. Del. Mar. 29, 2018). The tort of unfair competition overlaps substantially with tortious interference with prospective business relations. The elements of unfair competition are: (1) that the plaintiff has a reasonable expectancy of entering a valid business relationship; (2) that the defendant wrongfully interferes with that relationship; and (3) that the defendant thereby defeats the plaintiff's legitimate expectancy and causes him harm. *Ethypharm S.A. France v. Abbott Lab'ys*, 598 F. Supp. 2d 611, 618 (D. Del. 2009), *vacated on other grounds*, 707 F.3d 223 (3d Cir. 2013) (quoting *Total Care Physicians, P.A. v. O'Hara*, 798 A.2d 1043, 1057 (Del. Super. Ct. 2001)).

[28] Although it was not developed as part of the briefing on defamation, Booking.com elsewhere in its brief points to sufficient evidence to raise a genuine question for trial as to whether this speech was economically motivated. *See* Dkt. No. 372 at 37. In particular, Booking.com points to evidence that Ryanair's marketing strategy is to decrease the number of Ryanair flights booked via OTAs. *See* Hemann Decl. Exh. 18 (summarizing the communications plan to address OTA bookings); Hartnett Decl. Exh. P (listing digital customer verification as part of its strategy to "[g]et customers to make direct bookings on the Ryanair [sic] and not use OTAs"); Hartnett Decl. Exh. Q (describing Ryanair's anti-OTA strategy); Hartnett Decl. Exh. R (listing emails to customers who book through OTAs as one item "for the next round of OTA disruption.").

Ryanair argues that Booking.com cannot prevail on its tortious interference and unfair competition claims because Booking.com cannot demonstrate either that Ryanair acted wrongfully by sending the relevant emails to its customers or that Ryanair knowingly interfered with Booking.com's business relationships by addressing customers who booked through OTAs generally. Booking.com argues that genuine disputes of material fact preclude summary judgment on both elements.

i. Wrongful Conduct

Under Delaware law, tortious interference claims are limited by the defendant's right "to compete or protect his business interests in a fair and lawful manner." *Lipson v. Anesthesia Services, P.A.*, 790 A.2d 1261, 1285 (Del. Super. 2001) (citing *DeBonaventura v. Nationwide Mut. Ins. Co.*, 419 A.2d 942 (Del. Ch. 1980), *aff'd*, 428 A.2d 1151 (Del. 1981)). The plaintiff has the burden to prove that the alleged tortious interference constituted wrongful interference, as opposed to permissible competition. *Id.* at 1287. Whether the competitor used "wrongful means" turns on whether the competitor used tactics that are independently actionable. *See CGB Occupational Therapy, Inc. v. RHA Health Servs. Inc.*, 357 F.3d 375, 388 (3d Cir. 2004); *Com. Nat. Ins. Servs., Inc. v. Buchler*, 120 F. App'x 414, 419 (3d Cir. 2004).[29]

Ryanair argues that because it has a financial interest in having its customers book their flights directly through Ryanair, and because Ryanair risks violations of law if it cannot provide the legally required notifications to its customers who booked Ryanair flights on Booking.com, Ryanair's statements to customers were necessarily permissible for the purposes of its tortious interference claim. Booking.com responds that a genuine dispute of material fact precludes

[29] While the *CGB Occupational Therapy* court was applying Pennsylvania law, both Pennsylvania and Delaware follow the Second Restatement of Torts on this issue. *See Com Nat. Ins. Servs. Inc.*, 120 F. App'x at 419; *Lipson*, 790 A.2d at 1287.

summary judgment on this issue because Booking.com has adduced evidence that Ryanair's verification procedure, described in its emails to its customers, is part of an anti-OTA business strategy.

The relevant question is not whether Ryanair has an "anti-OTA business strategy," but whether Ryanair has used tactics that are unlawful. There is nothing inherently unlawful about Ryanair competing with OTAs or attempting to persuade passengers who book through OTAs to book with Ryanair directly instead. *See Buchler*, 120 F. App'x at 419 ("A competitor does not 'wrongfully interfere' with its competitor's at-will customers by simply competing for their business") (citing Restatement (Second) of Torts § 768). However, Ryanair's privilege does not authorize it to use unlawful tactics. Because I have held that Booking.com's defamation claim survives Ryanair's motion for summary judgment, there remains a factual dispute as to whether Ryanair implemented its strategy through improper means, in this case by defamatory statements. Whether Booking.com can ultimately carry its burden to establish wrongful means is a question of fact for the jury. *See Lipson*, 790 A.2d at 1287–88; *see also U.S. Bank Nat'l Ass'n v. Gunn*, 23 F. Supp. 3d 426, 436–37 (D. Del. 2014).

ii. Intentional Interference

Ryanair argues that it did not have the required degree of knowledge to intentionally interfere with Booking.com's prospective business relations by sending emails to suspected OTA customers. Dkt. No. 348 at 35–36 (citing *Shure Inc. v. ClearOne, Inc.*, No. CV 19-1343, 2021 WL 4894198, at *2 (D. Del. Oct. 20, 2021) ("It would be hard to 'intentionally interfere' with something that was not known."")). Ryanair argues that because OTAs conceal their identity to evade detection, Ryanair could not have known whether it was communicating with a

Booking.com customer when Ryanair sent emails to customers suspected of having used OTAs to book flights.

Ryanair determines based on various metrics (e.g., email addresses, payment details, and IP country of origin) that particular customers are likely to have used OTAs to book flights, but it does not know which OTA booked a particular customer's flights. *See* Fuga Decl. Exh. 26 at 32:15–34:22 ("[W]e don't know who each individual booking belongs to."); Fuga Decl. Exh. 29 at 42:18–43:9, 163:29–164:14 ("I don't know . . . who is the OTA behind that . . . they're all hiding now, and that's the challenge that we have."). Ryanair does not dispute that among the customers to whom it sends the "OTA emails" there are likely to be customers of Booking.com, but it argues that it sends those emails to particular customers because those customers have a booking that is flagged as an OTA booking, not because Ryanair knows that Booking.com is the OTA in a particular case.

Booking.com responds that there is sufficient evidence to show knowledge by Ryanair that some of the customers who receive its emails are likely to have booked their flights through Booking.com, or at least enough evidence to create a disputed question of fact on that issue. Booking.com cites Ryanair's internal records to show that Ryanair specifically targets Booking.com customers. *See* Hemann Decl. Exh. 18 (listing litigation against Booking.com as part Ryanair's "OTAs – Comms Plan"); Hartnett Decl. Exh. V (email and attachment listing Booking.com on Ryanair's "OTA Cheat Sheet"); Hartnett Decl. Exh. M (listing Booking.com as one of the OTAs selling Ryanair flights in Ryanair's OTA Review from August 2023); Hartnett Decl. Exh. CC (referring to Booking.com as an "OTA Pirate" on Ryanair's blog in January 2024).

Booking.com is correct that from those facts, a reasonable jury could infer that Ryanair knew Booking.com customers were among the OTA customers to whom it has sent emails. *See*

Shure, 2021 WL 4894198, at *3. In response, Ryanair asserts that in order to prevail on its intentional interference charge, Booking.com must be able to show not only that Ryanair had such knowledge but that Ryanair's "primary intent" in sending those emails was to target Booking.com customers specifically. *See* Dkt. No. 380 at 17 (citing *Buchler*, 120 F. App'x at 418–19).

That proposition misstates the applicable law. The *Buchler* court did not apply a "primary intent" test. Moreover, Delaware courts have explained that whether the defendant's motive was at least partly competitive is only one factor in determining whether an interference is improper and is not, by itself, dispositive. *See Beard Rsch., Inc. v. Kates*, 8 A.3d 573, 611 (Del. Ch.), *aff'd sub nom. ASDI, Inc. v. Beard Rsch., Inc.*, 11 A.3d 749 (Del. 2010); *Lipson*, 790 A.2d at 1287–88 (whether an interference is improper is a multi-factor inquiry that is "typically a question of fact for the jury"); *see also* Restatement (Second) of Torts, § 767. Ryanair is therefore not entitled to summary judgment of no intentional interference based on the absence of evidence of knowledge.

C. Damages

Ryanair argues that Booking.com's tortious interference, unfair competition, and trade libel claims fail because Booking.com cannot prove that it suffered a compensable injury as a result of Ryanair's emails to customers.

i. Admissibility of Customer Complaints

Booking.com seeks to rely on customer complaints about the emails its customers received from Ryanair, which led the customers to complain that Booking.com had acted improperly in the course of booking their flights. Ryanair responds that Booking.com's reliance on customer complaints is insufficient to establish that it has lost business and good will among customers. Ryanair first argues that Booking.com's customer complaints are inadmissible hearsay. In addition, Ryanair points out that many of the comments relied upon by Booking.com are

unauthenticated translations from languages other than English. And even if the customer complaints are admissible, Ryanair argues, Booking.com has made no showing that it suffered any pecuniary loss as a result of those complaints. To the contrary, Ryanair points out, the evidence shows that Booking.com's sales of Ryanair flights increased during the period at issue in this case.

In its brief, Booking.com responds that its customer complaints are admissible as business records under Federal Rule of Evidence 803(6), as evidence of the customer's then existing state of mind or emotional condition under Rule 803(3), or as the customer's present sense impressions under Rule 803(1). Booking.com also argues that the complaints are offered for a purpose other than for the truth of the matters asserted in the complaints; in particular, Booking.com argues that the complaints are admissible to show that customers were unhappy with Booking.com, thus supporting Booking.com's theory of economic reputational harm. Booking.com further notes that while the number of its Ryanair bookings have increased over time, the growth rate for its sales of Ryanair flights has been low relative to the growth rate for other sales, which supports its theory that it has suffered damages attributable to Ryanair's alleged acts of tortious interference, unfair competition, and trade libel.

During the hearing on the summary judgment motions, Booking.com withdrew its argument that customer complaints are admissible as business records under Rule 803(6) because Booking.com collects and maintains those complaints. Wisely so, as that argument was plainly wrong. To qualify as a business record under Rule 803(6), the record of an event must be one made in "the course of a regularly conducted business activity." Fed. R. Evid. 803(6); *see United States v. Pelullo*, 964 F.2d 193, 200 (3d Cir. 1992) (Rule 803(6) requires that "the declarant made the record in the regular course of the business activity"); *Rowland v. Am. Gen. Fin., Inc.*, 340 F.3d 187, 194–95 (4th Cir. 2003) (same); *United States v. Baker*, 693 F.2d 183, 189 (D.C. Cir. 1982)

(Rule 803(6) only applies if "every . . . participant in the chain producing the record" is acting in the regular course of business). Customer complaints are not business records, because the customer typically is not acting in the regular course of business activity when making the complaint. *See, e.g., Rowland*, 340 F.3d at 195; *Kendall v. Bausch & Lomb Inc.*, No. CIV. 05-5066, 2011 WL 860447, at *5 (D.S.D. Mar. 9, 2011) (customer complaints received by a party are not business records); *ADT LLC v. Alarm Prot. LLC*, No. 9:15-CV-80073, 2017 WL 1881957, at *2 (S.D. Fla. May 9, 2017) (same).

Even if the log of customer complaints kept by Booking.com is itself is a business record, the complaints present a double hearsay problem: a record of the receipt of complaints may be business records, but the customers' complaints are not. And the complaints themselves must be independently admissible for the contents of the complaints to be allowed into evidence. *See Rowland*, 340 F.3d at 195; *Salas v. Toyota Motor Sales*, No. 2:15-CV-08629, 2024 WL 1083078, at *4 (C.D. Cal. Feb. 2, 2024); *QVC, Inc. v. MJC Am., Ltd.*, No. CIV.A. 08-3830, 2012 WL 33026, at *2 (E.D. Pa. Jan. 6, 2012).

There is considerably more force to Booking.com's argument that complaints that specifically state an intention not to book flights through Booking.com in the future are admissible under Rule 803(3) as "[a] statement of the declarant's then-existing state of mind." *See, e.g.,* Hartnett Decl. Exh. W ("I have been advised by Ryanair that they have NO commercial relationship with booking.com and that the booking I have paid for has been blocked. . . . I have been a Genius level customer for years but no more."); Hartnett Decl. Exh. X ("I will never use booking.com to make a reservation again after this experience [booking a Ryanair flight through Booking.com]").

Such evidence is admissible under Rule 803(3) to show a customer's then-existing state of mind, including the customer's intent or plan. *See GF Princeton, L.L.C. v. Herring Land Grp., L.L.C.*, 518 F. App'x 108, 113 (3d Cir. 2013) ("Testimony as to customer motivation is admissible as an exception to hearsay under Fed. R. Evid. 803(3)"); *Callahan v. A.E.V., Inc.*, 182 F.3d 237, 251–52 (3d Cir. 1999) (same).[30]

Citing the Third Circuit's decision in *Callahan*, Ryanair argues that while the customers' complaints can be admitted to show the customers' intentions (such as the expressed intention to stop doing business with Booking.com), the complaints cannot be used to show that declarants acted in conformity with that expressed intent. That is a misreading of Rule 803(3) and Supreme Court and Third Circuit authority.

In *Mutual Life Ins. Co. v. Hillmon*, 145 U.S. 285 (1892), the Supreme Court held that a statement of the declarant's intent is admissible not only to show the declarant's intention, but also as evidence that he acted on that intention. The Advisory Committee note on Federal Rule of Evidence 803(3) made clear that the current rule embraces that holding. As the Advisory Committee wrote, "The rule of [*Hillmon*], allowing evidence of intention as tending to prove the

[30] Booking.com also argued in its brief that the customers' complaints were admissible under Federal Rule of Evidence 803(1), the exception to the hearsay rule for present sense impressions. The problem with that argument is that Booking.com has not offered any evidence that the declarations described or explained "an event or condition, made while or immediately after the declarant perceived it," which is a necessary condition for admission of a statement under that exception.

To the extent that customer statements do not go to the customers' state of mind, they are not admissible under Rule 803(3). As Booking.com argues, however, such statements are still admissible for the non-hearsay purpose of showing that customers complained to Booking.com following their receipt of emails from Ryanair. *See Allscripts Healthcare, LLC v. Andor Health, LLC*, No. CV 21-704, 2022 WL 17403121, at *1–2 (D. Del. Aug. 9, 2022) (customer complaints are not hearsay when offered as evidence that complaints were made rather than for the truth of what was complained about).

doing of the act intended, is, of course, left undisturbed." The Third Circuit has said the same thing. *See Kos Pharms., Inc. v. Andrx Corp.*, 369 F.3d 700, 719 (3d Cir. 2004) ("To the extent such statements address the speaker's plans . . . , they create an inference that the declarant acted in accord with that plan."); *United States* v. *Donley*, 878 F.2d 735, 737–38 (3d Cir. 1989) (same)); *see also Janssen Pharms., Inc. v. Tolmar, Inc.*, No. 21-1784, 2024 WL 834762, at *14-15 (D. Del. Feb. 26, 2024) (same).[31]

In any event, it is not necessary to probe the extent to which the customer complaints admitted under Rule 803(3) can be used to prove that the customers acted consistently with their expressed intentions and that Booking.com lost business as a consequence. That is because at the hearing on the summary judgment motions, Booking.com expressly disclaimed reliance on the customers' complaints to show that the customers in fact stopped doing business with Booking.com and that Booking.com suffered financial injury as a result. The court will hold Booking.com to that disclaimer.

Ryanair argues that several of the customer comments are inadmissible because they appear in a spreadsheet column titled "comments translated," and it is unclear how they were translated, whether those translations are accurate, and whether the comments are verbatim or paraphrased. *See* Fuga Decl. Exh. 31. Ryanair argues that under Federal Rule of Civil Procedure

[31] The *Callahan* case, the sole authority on which Ryanair relies on this issue, does not support Ryanair's contention. In that case, the Third Circuit explained that the admission of a statement of the declarant's intent or motives may not be admitted "as evidence of the facts recited as furnishing the motives." 182 F.3d at 252. That is simply a restatement of the well-established principle that while an out-of-court statement admissible as a statement of intent can be used as evidence that the declarant acted in the future consistently with his expressed intent, it cannot be used to prove events the past events that may have given rise to the declarant's intent or motive. As Justice Cardozo put it in the famous case of *Shepard v. United States*, 290 U.S. 96, 105–06 (1933), "Declarations of intention, casting light upon the future, have been sharply distinguished from declarations of memory, pointing backwards to the past."

56(e), Booking.com cannot rely on that evidence to survive the summary judgment motion because the translations were unauthenticated, and the comments were therefore inadmissible. But in its response to the summary judgment motion, Booking.com relies primarily on English language customer complaints. *See, e.g.,* Hartnett Decl. Exh. W; Hartnett Decl. Exh. X; *see also* Hartnett Decl. ¶¶ 33–34 (attesting that exhibits W and X are true and correct copies of customer service tickets); Second Guerrero Decl. ¶¶ 5–7 (certification of records, including customer emails).[32] Booking.com may rely on the English language emails for the purposes of responding to the summary judgment motion under Federal Rule of Civil Procedure 56(e); the translated complaints will not be taken into account in determining the disposition of Ryanair's summary judgment motion on this issue.

ii. Booking.com's Theory of Loss

In light of Booking.com's acknowledgement that it will rely on the customer complaints only for the limited purpose of proving the customers' state of mind, the question remains whether Booking.com has adduced sufficient evidence of damages to satisfy the damages element of its tortious interference, unfair competition, and trade libel claims.

Ryanair argues that Booking.com has not proved damages by showing that it has lost customers as a result of Ryanair's emails. To the contrary, Ryanair argues, Booking.com's sales of Ryanair flights have increased over the last several years. *See* Fuga Decl. Exh. 32 at 8, Exh. B. Moreover, Ryanair argues that Booking.com has provided no calculation of damages to sustain its burden. Rather, Ryanair maintains that the evidence Booking.com has adduced relating to

[32] Booking.com also provided information on how customer feedback in the spreadsheet was translated. *See* Second Guerrero Decl. ¶¶ 9–13. It appears that translations were done by an automated program. The court does not need to address whether this translation is sufficiently reliable because Booking.com relies primarily on English language customer complaints in its response to the motion for summary judgment.

damages is speculative and cannot sustain a finding that Booking.com has satisfied the damages requirements of the three economic torts. *See Beard Rsch*, 8 A.3d at 613.

Because Booking.com is not relying on customer complaints as evidence that any repeat customers stopped using the company's services, Booking.com relies on a theory of economic reputational harm. It argues that the complaints show harm to its reputation, and that such harm is pecuniary in nature. Booking.com points to the testimony of Mr. Guerrero, who testified that Ryanair's emails have adversely affected flight sales, and that Booking.com has suffered pecuniary harm as a result of that reputational harm. *See* Hartnett Decl. Exh. K at 248:8–260:14. In his deposition, Mr. Guerrero admitted it is "difficult to identify what is the real impact" of the emails, but he maintained that "reputation equals money." *See id.* at 249:19–251:4. In support of his contention that Booking.com has suffered a monetary loss due to that reputational injury, Mr. Guerrero also testified that [redacted]. *Id.* at 252:14–260:17.

Based on the Guerrero testimony and a calculation provided in Ms. Hartnett's declaration, *see* Hartnett. Decl. ¶¶ 4–8, Booking.com argues that it can prove injury and causation to the jury.[33] Booking.com argues its evidence is sufficient to create a genuine issue of fact as to damages because at this stage of the proceedings it need only establish that it suffered some damages, and is not required to show the quantum of damages. Dkt. No. 372 at 41 & n.18 (citing *Callahan*, 182

[33] In its reply brief, Ryanair asserts that those figures have never been produced before and that the calculation in Ms. Hartnett's declaration is incorrect. Regarding the former, Mr. Guerrero clearly referenced the difference in growth rates in his deposition testimony as evidence of lost profits or pecuniary harm. *See* Hartnett Decl. Exh. K at 252:14–260:17. Thus, Booking.com's theory of harm is not new. Whether the specific calculation in Ms. Hartnett's declaration is correct is an issue for cross-examination, assuming Booking.com introduces admissible evidence of the underlying figures as part of its case for damages.

F.3d at 247; *Beard Rsch.*, 8 A.3d at 612 (to establish liability, plaintiffs "need show only that they suffered some damage, not the precise amount of damage.").

Although the evidence on damages is thin, Booking.com has produced sufficient evidence to show that there is a genuine issue of fact as to whether it has suffered damages; the quantum of damages is appropriately addressed at a later stage of the case. [redacted] Ryanair is, of course, also correct that [redacted], such as its improved technological barriers. *See* Dkt. No. 380 at 19–20. However, whether Booking.com has shown [redacted] *See Lipson*, 790 A.2d at 1291 ("Generally, the issues of causation and damages are left for the jury.").

Ryanair relies primarily on *Beard Research* for its argument that Booking.com's evidence of damages is too speculative, and that Booking.com will be unable to provide a "responsible estimate of damages." 8 A.3d at 613. The court in that case explained that a court "may not set damages based on mere 'speculation or conjecture.'" *Id*. However, the procedural posture of that case was different from the procedural posture of this one: the court in that case was making post-trial findings of fact and conclusions of law. Thus, while it is true that Booking.com needs to provide an evidentiary basis from which the jury could make a responsible estimate of damages at trial, it would be premature to rule that Booking.com has not provided such a basis at this stage, when it has provided enough evidence to show that the fact of damage is in dispute. *Id.* ("The quantum of proof required to establish the amount of damage is not as great as that required to establish the fact of damage.") (citation omitted). Ryanair's motion for summary judgment is

therefore denied as it relates to Booking.com's tortious interference, unfair competition, and trade libel counterclaims.

iii. Defamation

In a footnote, Ryanair argues that Booking.com can, at most, seek only nominal damages for its defamation claim because it cannot show injury to its reputation in light of the inadmissibility of customer complaints. *See* Dkt. No. 348 at 36 n. 18 (citing *Preston Hollow Cap. LLC v. Nuveen LLC*, No. N19C-10-107, 2022 WL 2276599, at *4 (Del. Super. Ct. June 14, 2022)). Booking.com argues that because this is a defamation per se case, harm to reputation is presumed. In support, Booking.com cites *Marcone v. Penthouse Int'l Mag. for Men*, 754 F.2d 1072, 1078 (3d Cir. 1985). That case is not instructive, however, because it applied Pennsylvania law.

Under Delaware law, "statements which 'malign one in a trade, business, or profession' are '. . . slander *per se*.'" *See Preston Hollow Capital*, 2022 WL 2276599, at *3 (citation omitted). In such cases, Delaware law still requires that a plaintiff show injury to reputation. *Id.* at *4 (citing *Gannett Co. v. Kanaga*, 750 A.2d 1174, 1184 (Del. 2000). However, Ryanair is incorrect in asserting that Booking.com has no evidence of damage to its reputation. Booking.com's assertion relies on the assumption that the customer complaints are inadmissible in their entirety, when they are in fact admissible to show both that complaints occurred and that the complaining customers intended to stop using Booking.com. That evidence is sufficient to show injury to reputation. Ryanair's motion for summary judgment will therefore be denied, and Booking.com will be allowed to present evidence of defamation at trial.

V. Ryanair's Daubert Motions

A. Opinions of Jordan Rae Kelly

Jordan Rae Kelly, the defendants' cybersecurity expert, presents three opinions in her report: (1) that the Ryanair website is publicly available in that there is no barrier to accessing the website; (2) that Ryanair necessarily granted access to its website in order for on-line flight purchases to be made; and (3) that there is no evidence that the defendants caused harm to the Ryanair website. *See* Hemann Decl. Exh. 38. Ryanair argues that all three opinions should be excluded.

i. Ms. Kelly's Opinions on Access to the Ryanair Website

Regarding Ms. Kelly's opinion that the Ryanair website is public, Ryanair argues that (1) Ms. Kelly's definition of "public" should be excluded because it would confuse the jury; (2) Ms. Kelly ignored crucial information regarding how Shield functions; and (3) the methodology that Ms. Kelly used in testing how Shield operates is unreliable because her test used humans instead of automated software (i.e., bots), and Shield was not designed to be a barrier to humans. The defendants respond that Ms. Kelly's definition of what constitutes a "public website" is admissible because she relies on industry-recognized standards to support her conclusion. The defendants also dispute Ryanair's contention that Ms. Kelly ignored critical information about the Shield system.

Regarding Ms. Kelly's opinion that Ryanair "necessarily granted access to its website" for flight purchases, Ryanair argues that Ms. Kelly's opinion is unreliable because she relied on a self-serving distinction between "good bots" and "bad bots" [34] and, instead of addressing Ryanair's

[34] Ms. Kelly offered the opinion in her report that cybersecurity professionals often distinguish between "good" and "bad" bots because the term "bots" itself is a broad term that covers software that automates certain functions on a website. She explained that the distinction

internally developed Shield Software, she repeatedly referenced a different, external Shield program owned by a Singaporean company having no relationship to this case. The defendants dispute Ryanair's characterization of Ms. Kelly's report, arguing that she had adequate support for her good-bot/bad-bot distinction and that, while it is true that Ms. Kelly mistakenly referred to the external Shield software from a Singaporean company, she admitted that mistake in her deposition and analyzed Ryanair's internal Shield program as well.

While the parties focus on the merits of Ms. Kelly's analysis, the fundamental issue with Ms. Kelly's first two opinions is that both address the legal issue of whether defendants (by way of their vendors) access the Ryanair website or the myRyanair portion of that website without authorization. In light of the court's legal conclusions regarding whether the alleged access to the Ryanair website in this case would be without authorization, which will govern the jury's consideration of those issues, Ms. Kelly's first and second opinions would not satisfy the requirement under Federal Rule of Evidence 702 that an expert's specialized knowledge "will help the trier of fact to understand the evidence or to determine a fact in issue." *See* Fed. R. Evid. 702(a).

ii. Ms. Kelly's Opinion on Harm to the Ryanair Website

Ryanair argues that Ms. Kelly's opinion that there is no evidence of harm to the Ryanair website is unreliable because Ms. Kelly characterizes harm more restrictively than the CFAA does and, in doing so, may mislead the jury. *See* Dkt. No. 348 at 46–47 (citing Fed. R. Evid. 702; *Schneider ex rel. Est. of Schneider v. Fried*, 320 F.3d 396, 404 (3d Cir. 2003) ("Rule 702 requires that the expert testimony must fit the issues in the case . . . and assist the trier of fact"); Dkt. No.

is useful to explain how Ryanair attempts to prevent the use of bots on its websites. *See* Hemann Decl. Exh. 38 at 22–32.

380 at 23–24. The defendants respond that Ryanair's real concern is not with Ms. Kelly's methods but with her conclusion, which is a basis for cross-examination, not for exclusion. *See* Dkt. No. 372 at 47–48 (citing *Allscripts Healthcare, LLC v. Andor Health*, *LLC*, No. 21-704, 2022 WL 3021560, at *26 (D. Del. July 29, 2022)). The defendants also argue that the fact that Ms. Kelly did not address the full range of possible losses under the CFAA is not a basis for exclusion, but rather merely reflects that she did not anticipate all of Ryanair's theories of loss, including the theory of loss that Mr. Lopata set forth in his contemporaneously filed expert report for Ryanair. *See id.*

Ms. Kelly's opinion that Ryanair cannot attribute website slowdowns or website disruption to any particular OTA is relevant to the case as it goes to the central issue of loss and damage. Based on the deposition testimony of Ryanair's witnesses and Ms. Kelly's own analysis of Ryanair flights sold by the defendants, Ms. Kelly concluded that the defendants' actions could not have caused the harm that Ryanair claims. *See* Hemann Decl. Exh. 38 at 32–41. Her opinion on that issue is directly responsive to a theory of harm that Ryanair has advanced throughout this case: that the defendants' access to the website harms the "availability and/or usability" of the Ryanair website. *See* Dkt. No. 76 at ¶¶ 270–72. Ryanair is thus incorrect in asserting that Ms. Kelly's opinion is not relevant to any issues in this case.

Ryanair's argument that Ms. Kelly's opinion is misleading or unreliable because other harms are cognizable under the CFAA, such as loss from Ryanair's investigation into bot activity, fails to recognize that Ms. Kelly's testimony is directed to whether there was any harm *to the Ryanair website*, not to the scope of all losses cognizable under the CFAA. To the extent that Ryanair's argument is that Ms. Kelly should have considered additional sources or additional context surrounding the depositions that she relied upon, such arguments are best addressed

through cross-examination, not exclusion. *See Stecyk v. Bell Helicopter Textron, Inc.*, 295 F.3d 408, 414 (3d Cir. 2002) ("A party confronted with an adverse expert witness who has sufficient, though perhaps not overwhelming, facts and assumptions as the basis for his opinion can highlight those weaknesses through effective cross-examination"); *see also Allscripts Healthcare*, 2022 WL 3021560, at *26. However, in light of my rulings that only the myRyanair portion of the website is private, Ms. Kelly will be limited to testifying as to the harm or lack thereof related to requests on the myRyanair portion of the website.

B. Timothy O'Neil-Dunne

Timothy O'Neil-Dunne is the defendants' travel industry expert. His report provides background on the development of the travel industry, methods of booking consumer travel, a comparison of full-service and low-cost carriers, and a discussion of Ryanair's business model and the benefits provided by OTAs. *See generally* Hemann Decl. Exh. 39.

Ryanair argues that Mr. O'Neil-Dunne's testimony should be excluded for three reasons. First, Ryanair characterizes Mr. O'Neil-Dunne's report as providing only general background on (1) the direct and indirect purchasing of airline tickets, (2) the post-internet travel industry, (3) modern methods of booking travel, (4) the preferences of airlines, and (5) the purposes of OTAs and their benefits to customers. Dkt. No. 348 at 39. None of that background information, Ryanair argues, is relevant to either the CFAA claims or Booking.com's counterclaims, and it should therefore be excluded. Second, Ryanair argues that Mr. O'Neil-Dunne's discussion of Ryanair does not constitute expert evidence because Mr. O-Neil-Dunne is not qualified to address the nature of Ryanair's business. Third, Ryanair argues that Mr. O'Neil-Dunne's opinions are unreliable because he provides no supporting methodology or analysis.

The defendants respond, first, that Mr. O'Neil-Dunne's testimony is relevant to the interpretation of "authorization" in the CFAA because he will testify that conduct such as screen scraping is a "commonplace computer activity" for OTAs of the sort that Congress did not intend to criminalize under the CFAA. *See Van Buren*, 593 U.S. at 393. Second, the defendants argue that Mr. O'Neil-Dunne's opinion regarding the value of agent-supplied information in the travel industry goes to Ryanair's argument that OTAs provide "false" information. Third, the defendants argue that Mr. O'Neil-Dunne's opinion that myRyanair's login process serves a business purpose rather than a cybersecurity purpose is relevant to the case. Under the liberal standard of admissibility under Rule 702, the defendants argue that the whole of Mr. O'Neil-Dunne's testimony, as reflected in his report, should be admitted. *See Orbital Eng'g, Inc. v. Buchko*, 578 F. Supp. 3d 736, 740 (W.D. Pa. 2022) (citation omitted); *see also United States v. Schiff*, 602 F.3d 152, 173 (3d Cir. 2010); *United States v. Ford*, 481 F.3d 215, 219 (3d Cir. 2007).

For the same reason that Ms. Kelly's opinions going to authorization and authentication will not assist the jury in deciding issues of fact, the defendants cannot rely on Mr. O'Neil's opinion on screen scraping in section 7.2.1 of his report to address authorization. To the extent his opinion about the purpose of myRyanair is intended to address whether myRyanair is an authentication mechanism, his opinion will also be excluded.

However, Ryanair has not shown that the remainder of Mr. O'Neil-Dunne's report is irrelevant or unreliable. Ryanair does not contest that Mr. O'Neil-Dunne is an expert in the travel industry nor does it suggest that his opinions are irrelevant to the counterclaims. Even after the defendants argued that his testimony was relevant to the counterclaims, Ryanair continued to address only whether Mr. O'Neil-Dunne's testimony was relevant to its CFAA claims. *See* Dkt. No. 380 at 20–21. Mr. O'Neil-Dunne's discussion of Ryanair's model, the commercial purposes

of myRyanair, and the use of OTA-supplied information are all relevant to the counterclaims. In particular, his testimony regarding the use of non-traveler-supplied information, i.e., information supplied by an OTA, *see* Hemann Decl. Exh. 39 § 8.2.2, and the commercial purposes of myRyanair, *see id.* § 8.2.3, has the "potential to assist the trier of fact" in deciding the defendants' defamation claim. *See supra* section IV.A.

C. Basil Imburgia

Basil Imburgia is the defendants' rebuttal expert, whose reports are directed to responding to Mr. Lopata's testimony concerning loss under the CFAA. *See* Hemann Decl. Exhs. 44 (Rebuttal Report) & 45 (Supplemental Rebuttal Report). Mr. Imburgia asserts in his report (1) that the methodology Mr. Lopata used to calculate loss in his opening damages report is unreliable; (2) that it is unlikely that the defendants could be the cause of slowdowns and shutdowns on the Ryanair website given the relative volume of their bookings compared to all OTA bookings of Ryanair flights; and (3) that Mr. Lopata failed to properly allocate costs to the individual defendants. *See* Hemann Decl. Exh. 44 at ¶ 12.

Ryanair seeks to exclude Mr. Imburgia's report on three grounds: (1) Mr. Imburgia is not qualified to testify on matters related to the CFAA; (2) Mr. Imburgia's analysis is unreliable; and (3) Mr. Imburgia's conflation of "loss" and "damage" will mislead the jury.

i. Mr. Imburgia's Qualifications

Ryanair argues that while Mr. Imburgia is qualified as an accountant, he is not qualified on matters related to the CFAA because he has no experience with CFAA claims and no technical expertise in cybersecurity. *See* Dkt. No. 348 at 47–48. Ryanair argues that Mr. Imburgia's lack of experience affected his report because Mr. Imburgia applied general damages principles such

as the duty to mitigate costs and to prevent windfalls, principles that do not apply to the calculation of loss under the CFAA.

The defendants respond that this argument is baseless because Mr. Imburgia is not offered as an expert on the CFAA, and he therefore does not need prior experience in CFAA litigation to testify in this case. *See In re ConAgra Foods, Inc.*, 302 F.R.D. 537, 550-51 (C.D. Cal. 2014). In addition, the defendants argue that it is permissible for Mr. Imburgia to criticize Mr. Lopata's calculations without offering a theory of his own regarding how to calculate costs under the CFAA, *see Complaint of Borghese Lane, LLC*, No. 2:18-CV-00533, 2023 WL 3114851, at *3 (W.D. Pa. Apr. 27, 2023).

Mr. Imburgia is qualified to testify regarding Mr. Lopata's calculations of loss and damages. Mr. Imburgia's opinions are based on his expertise as an accountant, which is not challenged, not as a technical expert on the CFAA. Mr. Imburgia therefore may properly critique the methodology Mr. Lopata used to calculate Ryanair's costs and to allocate those costs to the defendants. *See Complaint of Borghese Lane, LLC*, 2023 WL 3114851, at *3 ("Courts have held that it is the proper role of rebuttal experts to critique [an] expert's methodologies and point out potential flaws in the . . . experts' reports.") (cleaned up) (collecting cases). The permissibility of Mr. Lopata's opinion on loss is addressed below, *infra* section IV.A.i, and a significant portion of that opinion is excluded. To the extent that Ryanair relies on the evidence underlying Mr. Lopata's report to make its case on loss and that evidence has the same problems that Mr. Imburgia raised in his criticism of Mr. Lopata's opinion on loss, Mr. Imburgia may testify to his rebuttal opinions. Mr. Imburgia need not have addressed loss under the CFAA in a prior trial in order to critique Mr. Lopata's analysis, or the underlying evidence, in the present case.

However, Ryanair is correct that to the extent Mr. Imburgia's criticisms are based on principles that do not apply to the calculation of loss for the CFAA, they are not proper rebuttals of Mr. Lopata's report. Accordingly, Mr. Imburgia may not testify that Mr. Lopata erred by failing to consider Ryanair's duty to mitigate, *see* Hemann Decl. Exh. 44 at ¶¶ 21–22, 70,[35] or that Mr. Lopata erred by failing to consider that Mr. Lopata's calculation method would result in a windfall for Ryanair, *id.* at ¶¶ 12 bullet point 3, 78.[36]

In addition, Mr. Imburgia is not qualified to testify about whether the defendants' actions are likely to have caused website slowdowns, because that question goes to a technical issue on which he is not qualified to testify. *See id.* at ¶¶ 12 bullet point 2, 76. Accordingly, his testimony corresponding to those paragraphs of his report will be excluded. However, Mr. Imburgia may testify in accordance with the portion of his report criticizing Mr. Lopata for not properly attributing an amount of harm from slowdowns or shutdowns to the defendants based on the facts in Mr. Lopata's report. *See, e.g.*, *id.* at ¶¶ 74–75.

ii. Reliability of Mr. Imburgia's Reports

Ryanair argues that Mr. Imburgia's reports and testimony are unreliable for two reasons. First, Ryanair argues that Mr. Imburgia's report is unreliable because he delegated much of the

[35] The defendants interpret Ryanair's argument on this issue as a criticism of Mr. Imburgia's analysis of Mr. Lopata's testimony regarding the costs of customer verification. *See id.* at ¶¶ 61–70; Hemann Decl. Exh. 45 at ¶¶ 19–24. Ryanair's criticism appears to be limited to paragraph 70 of Mr. Imburgia's report, which addresses the duty to mitigate, not Mr. Imburgia's criticism of how Mr. Lopata calculated the cost of customer verification. In any event, the latter criticism by Mr. Imburgia is admissible because it goes to Mr. Lopata's methodology and calculations rather than to an inapplicable concept such as the duty to mitigate, which is not relevant to the CFAA's loss provision.

[36] In the same sentence, Mr. Imburgia states that Mr. Lopata's contention that the defendants are liable for the total costs related all to OTA activities, despite the defendants being responsible for less than 3 percent of all OTA bookings is unreasonable. Mr. Imburgia may testify to this opinion, as it goes to his criticism of Mr. Lopata's failure to properly allocate costs to the defendants.

work on the report to other individuals. *See* Fuga Decl. Exh. 37 at 106:21–107:12, 108:17–109:3. As a result, Ryanair argues, Mr. Imburgia made the error of using revenue figures for the Ryanair Group, a holding group, in a calculation meant for Ryanair DAC, which operates the airline and website and is the plaintiff in the present case. *See* Hemann Decl. Exh. 45 at ¶¶ 30–32; Fuga Decl. Exh. 37 at 300:12–303:20. Second, Ryanair argues that Mr. Imburgia stopped his analysis at the "surface level of citations" in the Lopata Report. *See* Dkt. No. 348 at 49.

The defendants respond that Mr. Imburgia's opinions are reliable because an expert witness is permitted to use assistants in formulating his expert opinions, and Mr. Imburgia was sufficiently involved in preparing the report for him to testify to its contents, *see* Hartnett Decl. Exh. BB at 108:1–16. Regarding Mr. Imburgia's use of the holding group data and his analysis of Mr. Lopata's sources, the defendants argue that such criticism is best addressed through cross-examination. *See UGI Sunbury LLC v. A Permanent Easement for 0.4308 Acres*, No. 3:16-CV-794, 2021 WL 5140050, at *9 (M.D. Pa. Nov. 4, 2021); *Allscripts Healthcare*, 2022 WL 3021560, at *26.

"It is well recognized that an expert witness is permitted to use assistants in formulating his expert opinion." *See Shire Viropharma Inc. v. CSL Behring LLC*, No. CV 17-414, 2021 WL 1227097, at *21 n.13 (D. Del. Mar. 31, 2021) (cleaned up). So long as the expert was "directly involved in the research, analysis or drafting of the report, even with substantial assistance from a colleague or associate, his involvement in and knowledge of the report are matters of weight, not admissibility." *Lee Valley Tools, Ltd. v. Indus. Blade Co.*, 288 F.R.D. 254, 266 (W.D.N.Y. 2013). Ryanair has not shown that Mr. Imburgia was not directly involved in the analysis and drafting of the report, and the defendants point to Mr. Imburgia's testimony that his process was to outline the

report, share the outline with his colleagues, and then provide edits and rewrites. *See* Hartnett Decl. Exh. BB at 108:1–16.

Ryanair's best argument on this issue is that, based on his deposition testimony, it appears that Mr. Imburgia did not understand that the plaintiff is Ryanair DAC, not Ryanair Group. *See* Fuga Decl. Exh. 37 at 137:9–140:3; 303:17–20. It is unclear from his deposition testimony, however, whether Mr. Imburgia was confused about the relevant entity or merely misremembered the name of the plaintiff. *See id.* The defendants are correct that the error can be explored through cross-examination and is not a sufficient ground for excluding Mr. Imburgia's testimony altogether. In addition, the error is not an adequate basis for concluding that Mr. Imburgia was not sufficiently involved in drafting the expert report to require that his testimony be excluded on that ground.

Ryanair's criticism that Mr. Lopata's analysis stopped at the surface level of the Lopata Report's citations is also based on Mr. Imburgia's deposition testimony. *See id.* at 147:12–150:24. That testimony rebuts Ryanair's assertion that Mr. Imburgia looked only at surface level citations in the Lopata report, as Mr. Imburgia testified that he looked at the underlying documents that Mr. Lopata relied upon. *Id.* at 148:10–18. The fact that during his deposition Mr. Imburgia did not remember which particular documents Mr. Lopata examined does not suggest that Mr. Imburgia's report is unreliable. To the extent Ryanair believes that Mr. Imburgia misrepresented what documents Mr. Lopata reviewed, that criticism would also be best explored during cross-examination.

iii. The conflation of "loss" and "damages"

Ryanair's final argument regarding Mr. Imburgia is that Mr. Imburgia's opinion will not "help the trier of fact to understand the evidence or to determine a fact in issue" because Mr.

Imburgia confused the terms "loss" and "damage" under the CFAA. Fed. R. Evid. 702. Ryanair argues that this lack of precision will confuse the jury in its effort to determine whether the loss requirement for the CFAA is met. *See United States v. Merrill*, No. 08-20574, 2010 WL 3981158, at *8 (S.D. Fla. Oct. 8, 2010) (finding expert testimony that defined and applied terms in a way that conflicted with the relevant regulations was inadmissible). The defendants do not appear to have addressed this issue beyond making the general point that Mr. Imburgia's testimony would be "helpful to the finder of fact." *See* Dkt. No. 372 at 48.

Mr. Imburgia's report addresses the definition of loss in the Lopata Report and the CFAA. *See* Hemann Decl. Exh. 44 at ¶ 16.[37] Nonetheless, he uses the terms "damages" and "loss" interchangeably. That loose use of the terms creates the potential for confusion given the specific definition of loss in the CFAA. Nonetheless, any such confusion can be cured short of exclusion by requiring that Mr. Imburgia refer to "loss" in non-ambiguous terms and by excluding testimony that addresses theories that are relevant only to a damages analysis, such as the duty to mitigate, as discussed above. Although Mr. Imburgia improperly used the word "damages" in his report, the substance of his criticisms of how Mr. Lopata calculated loss (e.g., Mr. Lopata's inability to allocate costs to particular defendants) has the potential to assist the trier of fact in determining the crucial issue of whether the CFAA requirement that a plaintiff in a civil case show loss of at least $5,000 in a one-year period.

[37] Mr. Imbruglia does not address "damage" as defined in the CFAA, nor would it be appropriate given that damage is a technical term under the CFAA, specifically defined in the statute. *See* 18 U.S.C. § 1030(e)(8) ("[T]he term "damage" means any impairment to the integrity or availability of data, a program, a system, or information.").

VI. Booking.com's Daubert Motions

A. Opinions of Iain Lopata

Mr. Lopata is a technical expert for the defendants. Mr. Lopata submitted three reports in this case, all of which are at issue in the defendants' motion to exclude his testimony: (1) Mr. Lopata's Opening Report, Hemann Decl. Exh. 40; (2) Mr. Lopata's Amended and Supplemental Report, Hemann Decl. Exh. 41; and (3) Mr. Lopata's Rebuttal Report, Hemann Decl. Exh. 42. His opening report, as amended, provides opinions from a cybersecurity perspective regarding the barriers to access on the Ryanair website and how the defendants access that website. His reports also address the total amount of the loss to Ryanair caused by the defendants' online booking activities. Mr. Lopata's rebuttal report was offered in response to Jordan Rae Kelly's opening cybersecurity report.

The defendants argue that Mr. Lopata's loss and damages opinions should be excluded in full. They also argue that Mr. Lopata's cybersecurity opinions based on one of the tests he conducted should be excluded, as well as certain portions of his rebuttal report.

i. Mr. Lopata's Opinions on Loss under the CFAA

Section F of Mr. Lopata's Amended and Supplemental Report addresses his opinions on loss under the CFAA. In that section of his report, Mr. Lopata describes those categories of costs that he believes qualify as "losses" within the meaning of the CFAA, and he estimates the amount of those qualifying costs that Ryanair has spent on blocking OTA activity or repairing harm from OTA activity. He also allocates that amount to each defendant based on the percentage of OTA activity he attributes to that defendant. *See* Hemann Decl. Exh. 41 at ¶¶ 69–182.

The defendants urge that Mr. Lopata's opinion on "damages and loss" be excluded on the grounds that Mr. Lopata is not an expert on damages and that his methods are unreliable.

Regarding his expertise, the defendants first argue that Mr. Lopata's opinions on damages and loss should be excluded in full because Mr. Lopata admitted that he is not a damages expert, see Hemann Decl. Exh. 41 ¶ 28, and because he lacks the sort of expertise in accounting, finance, or economics that would be required for him to offer an expert opinion on this topic. *See Trs. of Univ. of Pa. v. Eli Lilly & Co.*, No. 15-6133, 2022 WL 3973276, at *3 (E.D. Pa. Jan. 14, 2022). They also argue that Mr. Lopata's opinion is a damages opinion in substance if not in name. *See Travelers Prop. Cas. Co. of Am. v. Hallam Eng'g & Constr. Corp.*, No. 08-0444, 2012 WL 13029519, at *3-4 (D.N.J. Aug. 16, 2012). As examples of his "damages" analysis, the defendants refer generally to Mr. Lopata's discussion of (1) joint and several liability, (2) allocation, and (3) whether Ryanair's losses exceed the statutory threshold.

In the alternative, the defendants argue that if Mr. Lopata is just doing simple math rather than conducting a damages analysis, he is not serving as an expert witness at all, because such calculations "are within the ken of a lay person." *Depalma v. Scotts Co.*, No. 13-7740, 2019 WL 2417706, at *7 (D.N.J. June 10, 2019); *Allscripts Healthcare*, 2022 WL 3021560, at *19 ("multiplication is not a specialized form of knowledge") (cleaned up).

Ryanair responds that Mr. Lopata is not offered as a damages expert but rather as a technical expert in cybersecurity who can properly provide an opinion as to which of Ryanair's costs should be classified as losses under the CFAA. Ryanair argues that the defendants' motion should be denied because it conflates two concepts: loss under the CFAA and legal damages. Mr. Lopata, Ryanair argues, has limited his testimony to the former category, based on his experience and expertise in information technology and cybersecurity. Additionally, Ryanair argues that Mr. Lopata is not simply performing basic arithmetic that a jury could perform but is using his

specialized knowledge to inform his opinion as to what constitutes a "reasonable cost" to a victim under the CFAA.

Section F of Mr. Lopata's report is directed to loss under the CFAA, not legal damages. He stated as much in his report. *See* Hemann Decl. Exh. 41 at ¶ 28. In addition, he clarified at his deposition that he is not offering an opinion on damages but instead is addressing "[t]he costs incurred by Ryanair in responding to unauthorized access to their website" based on his experience with "the financials of an [Information Technology] project." *See* Hemann Decl. Exh. 9 at 56:8–57:24. That Mr. Lopata is not a damages expert is thus irrelevant. The confusion about Mr. Lopata's report arises from the same problem that Ryanair pointed out in Mr. Imburgia's report: Mr. Lopata uses the term "damages" interchangeably with the statutory term "loss." *See, e.g.,* Hemann Decl. Exh. 41 at ¶¶ 25 ("I understand that whether the damages caused exceed $5,000 in a single year is an important threshold [issue]").[38] While Mr. Lopata use of those terms is imprecise, that imprecision can be cured.

The defendants are correct, however, that Mr. Lopata's expertise in information technology is not relevant to Mr. Lopata's ultimate calculations of loss. To the extent that Mr. Lopata is offering an opinion on what constitutes "loss" under the CFAA, Mr. Lopata's opinion would be an improper legal conclusion because it goes to the meaning of that term in the CFAA. *See Vox*

[38] The defendants' argument that in his discussion of joint and several liability and allocation Mr. Lopata's report addresses "damages" in all but name is incorrect. Mr. Lopata clearly disclaimed that he was offering an opinion as to the appropriate legal approach in this case. Instead, he summarized two approaches so that he could offer an opinion on loss under the CFAA under either approach. *See* Hemann Decl. Exh. 41 at ¶¶ 27(i)–(k), 153–155. His opinions thus do not run afoul of the problem in *Travelers Property Casualty Co.*, 2012 WL 13029519, at *3–4, cited by the defendants. The court in that case rejected an expert's opinion on the allocation of damages because the expert did not follow industry standards and could not articulate how he reached the apportionment figures that he did. *Id.*; *cf.* Hemann Decl. Exh. 41 at F.3 (describing Mr. Lopata's method for allocating costs to each defendant).

Mktg. Grp., LLC v. Prodigy Promos L.C., 521 F. Supp. 3d 1135, 1149 (D. Utah 2021) (excluding an expert report that offered "legal conclusions on terms contained in the [CFAA]"). Because the meaning of "loss" is a legal question, the question of which of Ryanair's costs may be considered a "loss" under the CFAA is addressed in the summary judgment opinion, *see supra* section III.B. In light of those rulings, Mr. Lopata may testify only on opinions he offered in his report as to which portions of certain systems can be allocated to preventing OTA activity.

For example, this court ruled that Ryanair may include the costs of CloudFront and AWS-WAF to the extent those costs are attributable to denying unauthorized bot requests by the defendants on the protected portion of the website. Accordingly, Mr. Lopata may offer his opinion as to which portion of the monthly cost for CloudFront and AWS-WAF is attributable to preventing OTA activity, based on his technical expertise. *See* Hemann Decl. Exh. 41 ¶¶ 98–103 (stating that CloudFront is multi-purpose, and that to the extent it serves purposes not used by OTAs, that portion of CloudFront costs cannot be allocated to OTAs).[39] Ryanair will still need to provide a way to allocate that portion of the costs to the defendants' activity on only the protected portion of the Ryanair website.

The bulk of Mr. Lopata's opinion on loss is directed to allocating the costs of Ryanair's various anti-bot measures to the defendants based on how much OTA activity goes through the

[39] At the hearing on the summary judgment motions, Ryanair's counsel argued that Mr. Lopata is doing more than simple math because he has brought his expertise to bear on what portions of certain costs are attributable to anti-bot activity. That is true with regard to this section of Mr. Lopata's report. It is also true with regard to his discussion of myRyanair costs, *id.* at ¶¶ 113–17, if Ryanair can show at trial that bot traffic attributable to the defendants has materially increased the cost of Ryanair's server infrastructure for the myRyanair portion of its website, *see supra* section III.B.i. The only other place where this appears to apply is Mr. Lopata's discussion of New Relic. Hemann Decl. Exh. 41 ¶¶ 104–112. Because of the ruling that the costs of New Relic are not losses under the CFAA, *supra* section III.B.i, Mr. Lopata's opinions based on those paragraphs will be excluded. The remainder of Mr. Lopata's estimates are unrelated to his technical expertise.

website and what percentage of OTA bookings are attributed to each defendant. This is simple math: Mr. Lopata uses Ryanair's estimate of the costs of a particular measure and multiplies that number by the percentage of a particular defendant's activity compared to all OTA activity on the website. To determine that amount, Mr. Lopata estimates what percentage of Ryanair's OTA bookings are attributable to each defendant based on the number of bookings each defendant reported. See, e.g., id. at ¶¶ 160–163 (calculation for Booking.com).

Such calculations are not based on Mr. Lopata's specialized knowledge. They represent the kind of chalkboard estimates based on other evidence in the case that Ryanair's counsel could equally well present in closing arguments. Courts in this district frequently reject exactly this kind of "calculation evidence" from experts because expert knowledge is not required to do simple arithmetic. *See Allscripts Healthcare*, 2022 WL 3021560, at *19 (excluding an expert's damages estimate created by merely multiplying values provided by the plaintiff, because no specialized knowledge was required to gather the input data and perform the calculation); *Cavi v. Evolving Sys. NC, Inc.*, No. CV 15-1211, 2018 WL 2317594, at *2 (D. Del. May 21, 2018) (excluding analysis that "amounts to nothing more than a simple math equation"); *CareDx, Inc. v. Natera, Inc.*, No. CV 19-662, 2021 WL 1840646, at *3 (D. Del. May 7, 2021) (same). Ryanair asserts that the calculation should be permitted because it is just a final step in Mr. Lopata's analysis. But if the rest of his proposed testimony is excluded, the calculation stands alone and must be excluded as well.

In sum, Mr. Lopata's opinions on the loss attributable to all OTA activity generally and to each defendant specifically is excluded because that evidence does not require specialized knowledge. In light of this ruling, there is no need to address the defendants' remaining arguments about the reliability of Mr. Lopata's method of calculating loss. Ryanair may attempt to introduce

the underlying evidence during the trial to make its argument that the CFAA's loss threshold is met. *See Cavi*, 2018 WL 2317594, at *2. But Mr. Lopata's testimony adds nothing to that evidence other than an exercise in arithmetic, and his testimony on that subject will therefore be excluded.

ii. Mr. Lopata's Opening Cybersecurity Opinions

Section E of Mr. Lopata's report contains his cybersecurity opinions, including a report of the testing Mr. Lopata performed to confirm whether the defendants accessed the Ryanair website to book flights and whether they circumvented protections on the Ryanair website to do so. *See* Hemann Decl. Exh. 41 ¶¶ 30–68. In the course of preparing his report, Mr. Lopata performed two tests. The first, Test A, was directed at determining whether Ryanair can accurately and reliably determine how a specific booking was made and whether the defendants use a Global Distribution System ("GDS")[40] or the Ryanair website to place bookings for Ryanair flights. *Id.* ¶¶ 39–40, 42. The second, Test B, was directed at determining, for bookings made through the Ryanair website, "whether these bookings are made through end-user interface or by direct access to the API." *Id.* ¶¶ 41–42. Direct access to the website's API is also referred to as "programmatic access."[41]

The defendants argue that the court should exclude Mr. Lopata's opinions related to Test B because Mr. Lopata conceded that his test failed, *see* Mao Decl. Exh. 7 at 201:2–5, 204:10–12, 207:2-21. In particular, the defendants seek to exclude Mr. Lopata's opinions regarding Test B set forth in paragraphs 27(c)-(e), 29, 31, 38–68, and 70 of his report, *see* Hemann Decl. Exh. 41,

[40] A GDS is a centralized booking tools for travel bookers, such as travel agents. *See* Hemann Decl. Exh. 39 at 7. Ryanair enters agreements with certain GDS companies to make its flights available on that company's GDS. *See* Fuga Decl. Exh. 1 at 74.

[41] An API connection allows two applications to communicate with one another. [redacted]

on the ground that they are not supported by a reliable methodology. *See In re TMI Litig.*, 193 F.3d 613 (3d Cir. 1999), *amended*, 199 F.3d 158 (3d Cir. 2000) (upholding the exclusion of expert opinion based on a flawed methodology); *In re Paoli R.R. Yard PCB Litig.*, 35 F.3d 717, 746 (3d Cir. 1994). The defendants also argue that Mr. Lopata has not shown that his testing methodology is a valid, industry-accepted means for determining programmatic access, and that his opinions should be excluded for that reason as well.

Ryanair responds that the defendants have mischaracterized Mr. Lopata's deposition testimony by describing it as a concession that Test B failed. At most, Ryanair argues, the cited testimony establishes that a single test booking did not conclusively show programmatic access, even though Mr. Lopata maintained that the access in that instance was mostly likely programmatic. *See* Mao Decl. Exh. 7 at 192:17–207:21. In addition, Ryanair argues that analysis of the defendants' PNR codes confirms Mr. Lopata's hypothesis that the defendants' bookings were made through programmatic access. *See* Fuga Decl. Exh. 6 at 83–84. And even if this court finds Test B unreliable, Ryanair argues, the defendants' request to exclude Mr. Lopata's testing evidence completely is too broad because it would result in excluding his testimony regarding Test A, which was not affected by the problems with Test B.

Test B involved [redacted]. Hemann Decl. Exh. 41 ¶¶ 63–68. Mr. Lopata then attempted to book that flight through the defendants' platforms. *Id.* Mr. Lopata stated that [redacted] *Id.* ¶ 64. At his deposition, Mr. Lopata was asked about one Test B test booking. For that booking, Mr. Lopata testified that he successfully submitted a booking

on the Booking.com website while [redacted] *See* Mao Decl. Exh. 7 at 192:17–209:1. When questioned, Mr. Lopata conceded that in light of those details, he could not conclude with confidence whether [redacted] *Id.* at 201:2–21. He went on to testify that [redacted] *Id.* at 202:21–204:24. He conceded, however, that counsel's questioning at the deposition would require him to clarify the opinion he set forth in paragraph 64 of his report. *Id.* at 207:2–21.

The full context of Mr. Lopata's testimony provides support for Ryanair's position that Mr. Lopata did not concede that Test B failed, but rather maintained his opinion that the defendants [redacted]. The deposition testimony demonstrates that there are limits to Mr. Lopata's testing methodology, limits that can be explored during cross-examination. However, the challenges to Mr. Lopata's testimony do not rise to the level of showing that Mr. Lopata lacks "good grounds" for his conclusion. *See In Re Paoli R.R. Litig.*, 35 F.3d at 746 ("[T]he judge should not exclude evidence simply because he or she thinks that there is a flaw in the expert's investigative process which renders the expert's conclusions incorrect. The judge should only exclude the evidence if the flaw is large enough that the expert lacks 'good grounds' for his or her conclusions."). However, Mr. Lopata's opinion will be limited to reflect the clarification he made at his deposition regarding the last sentence of paragraph 64 (i.e., that Test B is not definitive on this point, although he maintains his opinion that [redacted]).

This case is unlike the Third Circuit case cited by the defendants, *TMI Litigation*, in which an expert did not modify his hypothesis after his own testing undermined that hypothesis. 193 F.3d at 675–76. Unlike in that case, Mr. Lopata's testing did not undermine his hypothesis; it merely showed that his conclusion was not as definitive as he had initially represented, because he had not considered a possible alternative explanation for the results of the test, an explanation that was explored at his deposition. *See* Mao Decl. Exh. 7 at 205:1–207:1. Mr. Lopata went on to say he would modify his opinion based on that possibility. *Id.* at 207:2–21. Requiring Mr. Lopata to testify to that modification will resolve the issue in the present case without requiring the exclusion of testimony that could help the trier of fact determine the issue of access.

iii. Mr. Lopata's Rebuttal Report

The defendants argue that three portions of Mr. Lopata's Rebuttal Report should be excluded. Having determined that Ms. Kelly may testify only regarding her third opinion, *see supra* section V.A, only the portions of Mr. Lopata's rebuttal report regarding Ms. Kelly's third opinion will be admitted. The defendants' first argument, that Mr. Lopata's discussion of Test A in paragraph 42 of his rebuttal report should be excluded, is therefore moot.

The defendants' remaining objections relate to the portion of Mr. Lopata's report addressing Ms. Kelly's third opinion regarding harm to the Ryanair website. The defendants argue that paragraphs 9(c)(ii) and 112–24 of Mr. Lopata's report is improper rebuttal, as it impermissibly introduced new theories and evidence unresponsive to Ms. Kelly's opinion. *See* Dkt. No.335 at 45 (citing *Withrow v. Spears*, 967 F. Supp. 2d 982, 1001–02 (D. Del. 2013); *Boles v. United States*, No. 1:13CV489, 2015 WL 1508857, at *2 (M.D.N.C. Apr. 1, 2015); *Bradley v. Amazon.com, Inc.*, No. 17-1587, 2023 WL 2574572, at *5 (E.D. Pa. Mar. 17, 2023)). The defendants argue that any reference to KAYAK's referral or link-out bookings and retries (i.e., multiple efforts by a bot to

book a flight) is improper because Mr. Lopata did not mention those subjects in his opening report. In addition, they argue that Mr. Lopata's new availability testing at paragraphs 115–24 is unreliable because (1) the method underlying the testing is not explained, (2) Mr. Lopata was not involved in the execution of the test, and (3) in his deposition Mr. Lopata relied on what Booking.com characterizes as "Googling and guessing to come up with what should be precise numbers." Dkt. No. 335 at 46. Accordingly, the defendants argue, Mr. Lopata's conclusions are merely speculative and must be excluded. *See Heller v. Shaw Indus., Inc.*, 167 F.3d 146, 159 (3d Cir 1999).

Ryanair responds that Mr. Lopata's references to KAYAK's link-out bookings and retries were proper, and that it would be unjust to hold that Mr. Lopata should have raised the issue earlier when he was precluded from doing so because KAYAK delayed producing the pertinent data. In any event, Ryanair argues that it was permissible for Mr. Lopata to introduce new theories or evidence since they were responsive to Ms. Kelly's report. *See Haskins v. First Am. Title Ins. Co.*, No. CIV.A. 10-5044, 2013 WL 5410531, at *4 (D.N.J. Sept. 26, 2013). Moreover, Ryanair contends that Mr. Lopata was merely pointing out flaws in Ms. Kelly's opinion, not introducing new theories. As for Mr. Lopata's testing summarized at paragraphs 115–24 of his report, Ryanair addresses the defendants' concerns with that material only briefly, arguing only that the jury should decide the credibility and weight of his testimony.

Mr. Lopata's testimony regarding KAYAK's link-out booking data and retries is admissible. As to the former, Mr. Lopata explained in his report that not all defendants included referrals in their initial responses, but that recent disclosures showed those numbers to be far higher than the figures on which Ms. Kelly relied. *See* Hemann Decl. Exh. 42 ¶ 113. As Ryanair argued, and the defendants do not dispute, the data Mr. Lopata relied on was not provided by the defendants

until after the close of discovery, and it was directly pertinent to Ms. Kelly's testimony. It was therefore proper for Mr. Lopata to use that new evidence to critique Ms. Kelly's conclusions. *See Withrow*, 967 F. Supp. 2d at 1001 ("[R]ebuttal . . . reports may cite new evidence and data so long as the new evidence and data is offered to directly contradict or rebut the opposing party's expert.") (quotation marks omitted).

Mr. Lopata's opinion that Ms. Kelly should have considered retries is similarly admissible. Mr. Lopata criticized Ms. Kelly's report for not considering that the defendants sometimes need to make multiple attempts in order for a booking to succeed, citing his own report for examples. Hemann Decl. Exh. 42 ¶ 114 (citing Hemann Decl. Exh. 41 at 36). In his opening report, he stated that repeated attempts "place[] additional demands on Ryanair's systems." Hemann Decl. Exh. 41 at 36 n.63. The opinion in Mr. Lopata's rebuttal report is thus not new, and the expansion on his opening report is permissibly responsive to Ms. Kelly's report.

Mr. Lopata's availability testing addresses the frequency with which the defendants accessed the data on Ryanair's prices, flights, and timetables. *See* Hemann Decl. Exh. 42 at 115–24. There is no need to address the parties' dispute over whether Mr. Lopata's availability testing was new or unreliable because it was directed only to the issue of access to the general Ryanair website, not to bookings on myRyanair. In light of my ruling that the Ryanair website is a public website, Mr. Lopata's availability testing is not relevant. And in light of the limitations on Ms. Kelly's opinion, it will not be necessary.

B. Opinions of Anthony Vance

Anthony Vance is Ryanair's technical expert who was retained to rebut the testimony of the defendants' technical expert, Mr. O'Neil-Dunne. Dr. Vance represented his background and expertise to be in the field of cybersecurity. *See* Hemann Decl. Exh. 43 at 3. Section VI of Dr.

Vance's report addresses what he regarded as the flaws in Mr. O'Neil-Dunne's opinions: (1) he criticized Mr. O'Neil-Dunne's failure to address the CFAA claims; (2) he criticized Mr. O'Neil-Dunne's failure to distinguish between authorized and unauthorized access by OTAs; (3) he discussed the technical measures employed by Ryanair to prevent OTAs from accessing the Ryanair website; (4) he criticized Mr. O'Neil-Dunne's failure to address harms or costs of OTAs; (5) he discussed those harms; (5) he discussed what he considered the "net costs" of OTAs; and (6) he criticized Mr. O'Neil-Dunne for not differentiating between licensed and unlicensed OTAs. *Id.* at 5–21. Sections VII–XII of Mr. Vance's report address particular sections of Mr. O'Neil-Dunne's report. *Id.* at 21–26.

The defendants argue that Dr. Vance's report should be excluded in full on the ground that it is unresponsive to Mr. O'Neil-Dunne's report and is therefore best characterized as an untimely opening expert report. In the alternative, the defendants argue that to the extent that Dr. Vance's report is in the form of rebuttal, the various opinions Dr. Vance sets forth in his rebuttal report are inadmissible under Federal Rule of Evidence 702 and the *Daubert* decision.

i. Proper Rebuttal Testimony

The defendants contend that in his rebuttal report Dr. Vance improperly offered opinions on cybersecurity issues that should have been presented in an opening report and are not responsive to Mr. O'Neil-Dunne's opinions as a travel industry expert. *See* Dkt. No. 335 at 47–49 (citing *Withrow*, 967 F. Supp. 2d at 1001–02; *Bradley*, 2023 WL 2574572, at *5). The defendants take particular issue with Dr. Vance's discussion of authorized and unauthorized access in section VI.B of his report, his opinion on technical barriers and hacks in section VI.C of his report, and his discussion of "costs" and "net costs" to Ryanair in sections VI.D and VI.E of his report. As such,

the defendants argue that Dr. Vance's report should be rejected as an untimely opening expert report. *See Bradley*, 2023 WL 2574572, at *14–15.

Ryanair responds that Dr. Vance's testimony is permissible rebuttal in that it will "explain, repel, counteract, or disprove the evidence of the adverse party." *See Crowley v. Chait*, 322 F. Supp. 2d 530, 551 (D.N.J. 2004). Ryanair argues that because Mr. O'Neil-Dunne addressed issues such as screen scraping and the impact of OTA activities, Dr. Vance was properly offered as a cybersecurity expert who could rebut Mr. O'Neil-Dunne's presentation of the "benefits" provided by OTAs. *See* Dkt. No. 376 at 45–47. In the alternative, Ryanair argues that if the court regards Dr. Vance's testimony as improper rebuttal, his testimony based on the report should be admitted even though the report may be viewed as untimely. Ryanair's argument for admitting Dr. Vance's testimony even if his report is regarded as belatedly produced, is based on the Third Circuit's familiar five-factor test set forth in *Meyers v. Pennypack Woods Home Ownership Association*, 559 F.2d 894, 904–05 (3d Cir. 1977) ("*Pennypack"*).

In light of the ruling that much of Mr. O'Neil-Dunne's report and proposed testimony is proper expert evidence regarding the defendants' counterclaims, Dr. Vance may testify to relevant opinions rebutting Mr. O'Neil-Dunne. But the opinions in section VI.A of his report (that Mr. O'Neil-Dunne did not address the CFAA) and in section VI.C of the report (that the defendants use "technical hacks" to bypass various Shield endpoints and myRyanair), are not relevant rebuttal opinions, as they are not addressed to Mr. O'Neil-Dunne's testimony and go to the question of unauthorized access. Those opinions are excluded, with the exception of Dr. Vance's opinion that myRyanair is intended to prevent OTA bookings. That opinion may be introduced to rebut Mr. O'Neil-Dunne's testimony that myRyanair is used primarily for personalization of customers for business purposes. Regarding Ryanair's argument that such opinions are permissible even though

they are untimely, there is no need to evaluate the *Pennypack* factors that might allow the opinions to be admitted despite the untimeliness of the reports on which they are based, because the excluded opinions go to the legal question of authorization rather than to a fact question for the jury and therefore would be inadmissible even if they had been timely presented.

Nonetheless, most of Dr. Vance's opinions set forth in sections VI.B, VI.D, VI.E, and VI.F of his report are admissible because they "repel, counteract, or disprove" evidence on the same subject by the defendants' expert. *See Withrow*, 967 F. Supp. 2d at 1001–02. To the extent that Mr. O'Neil-Dunne's testifies regarding the benefits of OTAs and their practices, Dr. Vance can testify as to his opinions that address the harms caused by OTAs that Mr. O'Neil-Dunne did not consider.

Section VI.B of Dr. Vance's report addresses unauthorized and authorized access to the Ryanair website. The bulk of Dr. Vance's criticisms rely on "authorization" as defined by a website's terms of use or terms of service. Dr. Vance can testify to his opinions that address Ryanair's terms of use to provide context for his opinions on the harms of OTAs. However, Dr. Vance must be clear that he is referring to a violation of the terms of use, not to the meaning of "authorization" under the CFAA. Dr. Vance may not testify regarding the opinion set forth in the paragraph of VI.B that discusses the CFAA, *see* Hemann Decl. Exh. 43 at 7.[42] To avoid confusion, Dr. Vance should testify regarding access contrary to the terms of use, rather than "unauthorized" access.

[42] Dr. Vance repeatedly testified in his deposition that he was not offering an opinion on whether access is authorized or unauthorized under the CFAA but rather that he was using those terms as they are used in his field. *See* Mao Decl. Exh. 13 at 39:25–40:7; 47:15–21; 69:17–21. Dr. Vance's reference to authorization creates the potential for confusion. That risk, however, is best addressed by requiring Dr. Vance to testify about access in violation of the terms of use or in violation of Ryanair's cease-and-desist letters, rather than by referring to "unauthorized access."

Sections VI.D, VI.E, and VI.F of Dr. Vance's report address harms or costs associated with access by OTAs in violation of Ryanair's terms of use. Testimony based on those sections of the report is admissible to rebut Mr. O'Neil-Dunne's discussion of the benefits of OTAs. As part of Dr. Vance's discussion of the harms caused by OTAs, his report discusses screen scraping and cites previous blog posts by Mr. O'Neil-Dunne that are critical of screen scraping. *See id.* at 14–19. The defendants argue that such testimony is not proper rebuttal because it does not respond to Mr. O'Neil-Dunne's report, but instead responds to Mr. O'Neil-Dunne's deposition, where he was asked about why he did not discuss the negative features of screen scraping despite having authored blog posts on that topic. *See* Dkt. No. 378 at 25 (citing *DOCA Co. v. Westinghouse Elec. Co., LLC*, No. 04-1951, 2011 WL 12896754, at *1 (W.D. Pa. Dec. 7, 2011) ("[T]he Federal Rules contemplate that the determination as to whether a rebuttal expert report is necessary be based on the opposing party's expert report – not the expert's deposition.")). However, Mr. O'Neil-Dunne's discussion of screen scraping appears in his opening report, not just in his deposition. *See* Hemann Decl. Exh. 39 § 7.2.1. For that reason, the discussion of screen scraping in Dr. Vance's report is proper, including his reference to Mr. O'Neil-Dunne's prior blog posts on that subject.

Dr. Vance's opinions discussed above are based on his cybersecurity experience. Given the overlap between the technical and business issues in this case (such as whether the purpose of myRyanair's restrictions on screen scraping is primarily competitive or primarily serves a security purpose), Dr. Vance's rebuttal is proper even though his expertise is not the same as Mr. O'Neil-Dunne's. Mr. O'Neil-Dunne similarly discussed technical issues, such as screen scraping, as they relate to the travel industry.

Sections VII–XII of Dr. Vance's report apply Dr. Vance's criticisms developed in section VI to particular sections of Mr. O'Neil-Dunne's report. Dr. Vance may testify based on the portions of his report that constitute permissible rebuttal testimony, as described above.

ii. Rule 702 and *Daubert*

The defendants argue that Dr. Vance's report does not satisfy the requirements of Rule 702 and *Daubert* for three reasons. First, the defendants argue that Dr. Vance lacks specialized knowledge of the travel industry. As a result, they contend, the court should exclude Dr. Vance's opinions (1) that Ryanair offers licenses on reasonable terms; (2) that "Ryanair has a very different business model compared to that of OTAs;" and (3) that inviting customers to personalize their myRyanair accounts does not make Ryanair a competitor of the OTAs. *See* Hemann Decl. Exh. 43 at 5, 25. Ryanair responds that Dr. Vance's opinion on licensing and competition between Ryanair and the OTAs do not require an expert. Ryanair also contends that Dr. Vance has expert knowledge of the travel business because he teaches at a business school and offered his opinions as an expert on that subject. *See* Hemann Decl. Exh, 10 45:14–19.

Dr. Vance's opinions regarding Ryanair's licensing fee and whether Ryanair and the OTAs are competitors are excluded as falling outside the field of Dr. Vance's expertise. Ryanair's argument that such opinions do not require an expert cut against Ryanair, as they show that Dr. Vance's opinions in this area are not based on specialized knowledge that would help the trier of fact understand the evidence or determine an issue of fact. *See* Fed. R. Evid. 702(a). Nor has Ryanair shown that Dr. Vance is an expert in the relevant field.

Ryanair offered Dr. Vance as an expert in cybersecurity. In that capacity, he teaches at a business school and advises businesses on cybersecurity measures. *See* Hemann Decl. Exh. 43 at 3. The only representation regarding his "business" expertise is found in a single exchange with

counsel at his deposition. Speaking about the harms of screen scraping, Dr. Vance testified that, "As a business professional, it's incomplete to consider benefits without also considering costs." He was then asked, "Are you opining in this case as a business professional expert?" to which he responded, "I'm a business professor, and so yes, I am. I'm a business professor and a cybersecurity professor, and I think both views are relevant for my report." Hemann Decl. Exh. 10 at 45:11–19. That exchange is not sufficient to show that Dr. Vance has relevant expertise to offer the business-related opinions that he offered.

Second, the defendants argue that Dr. Vance improperly relied on Ryanair's allegations as true. *See id.* at 8 & n.16, 13 & n.35. Ryanair responds that Dr. Vance did not simply rely on Ryanair's allegations, but considered numerous documents including interrogatories, produced documents, Mr. Lopata's report, third-party resources. In addition, Dr. Vance relied on his own expertise. *See id.* at App'x B (listing documents Dr. Vance consulted).

The defendants have not shown that Dr. Vance improperly relied on Ryanair's allegations as true. The only references the defendants offer in support of that contention are the portions of Dr. Vance's report at footnotes 16 and 35, along with the accompanying text. Footnote 16 is a citation to Ryanair's cease-and-desist letters, which were attached to the complaint and which both parties agree the defendants received. Footnote 35 is a citation to a reference to myRyanair in the complaint, which is followed by citations to interrogatory responses and deposition testimony. As is evident in that footnote, Ryanair is correct that Dr. Vance did not simply rely on allegations in the complaint to form his opinions.

Third, the defendants argue that Dr. Vance's proposed testimony is improperly directed to (1) the meaning of authorization under the CFAA, *see id.* at 6–7, 21, 16 n.49; (2) the relevance of Mr. O'Neil-Dunne's testimony, *id.* at 5–6, 21; and (3) the meaning of the contractual provision

setting forth Ryanair's terms of use, *id.* at 7, 12, 14, 24.[43] Ryanair responds to only the first argument. In that response, Ryanair disputes that Dr. Vance offers a legal conclusion regarding authorization under the CFAA based on Dr. Vance's representations in his deposition that he was referring to authorization as a security term, not a legal term. *See* Mao Decl. Exh. 13 at 39:25–40:7; 47:15–21; 51:25–52:2; 69:17–21; 176:6–25. As addressed previously, Dr. Vance's opinions on "authorization" under the CFAA as well as the relevance of Mr. O'Neil-Dunne's report will be excluded, which renders the first two issues moot.

The remaining issue is whether Dr. Vance may offer his opinions that relate to the terms of use on the Ryanair website. At page 12 of his report, Dr. Vance stated that Ryanair is justified in taking action against OTAs that violate its terms of use. The terms of use are clear and do not require interpretation. The defendants' argument that they do not violate Ryanair's terms of use is based on their contention that they do not access the Ryanair website, either directly or vicariously. Dr. Vance will be allowed to testify that an OTA that accesses the Ryanair website to sell Ryanair flights without a license or to extract data for commercial purposes would violate Ryanair's terms of use. It will be up to the jury to decide whether the defendants do so, if the jury concludes that question is relevant to any issue in the case..

CONCLUSION

In summary, the court's rulings are as follows:

1. Ryanair's motion for summary judgment on Counts I and IV is denied.

2. Ryanair's motion for summary judgment dismissing Booking.com's counterclaims is denied.

[43] The defendants also include a criticism of Dr. Vance based on an expert report of his that was excluded in a different case. That criticism has no bearing on the motion to exclude his testimony in this case.

3. Ryanair's motion to exclude the testimony of Mr. O'Neil-Dunne is denied.

4. Ryanair's motion to exclude the testimony of Ms. Kelly is granted in part and denied in part.

5. Ryanair's motion to exclude the testimony of Mr. Imburgia is granted in part and denied in part.

6. The defendants' motion for summary judgment on Ryanair's claims under the CFAA is granted in part and denied in part.

7. The defendants' motion to exclude certain opinions of Mr. Lopata is granted in part and denied in part.

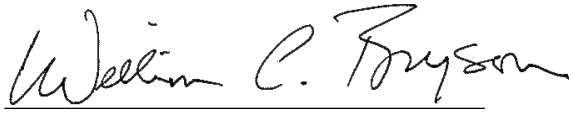
8. The defendants' motion to exclude the opinions of Mr. Vance is granted in part and denied in part.

* * *

The parties have filed all briefing on these motions and the supporting declarations under seal. Out of an abundance of caution, I have filed this order under seal. Within three days, the parties are directed to advise the court by jointly submitted letter if there are any portions of this order that should remain under seal and, if so, to explain why. An unsealed version of this order will be docketed after counsel's letter is received.

IT IS SO ORDERED.

SIGNED this 17th day of June, 2024.



WILLIAM C. BRYSON
UNITED STATES CIRCUIT JUDGE