UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

FACEBOOK, INC., et al.,

Plaintiffs,

v.

ONLINENIC INC, et al.,

Defendants.

Case No. 19-cv-07071-SI (SVK)

ORDER GRANTING AS MODIFIED PLAINTIFFS' MOTION TO STRIKE DEFENDANTS' ANSWER AND FOR DEFAULT JUDGMENT AGAINST DEFENDANTS ONLINENIC AND DOMAIN ID SHIELD

Re: Dkt. Nos. 176, 183, 185, 188, 194, 201, 206

Plaintiffs Facebook, Inc. and Instagram LLC ("Plaintiffs") move to strike Defendants OnlineNIC Inc. ("OnlineNIC") and Domain ID Shield Service Co.'s ("ID Shield") (together, "Defendants") Answer (Dkt. 88; Dkt. 108) and for default judgment against Defendants OnlineNIC and ID Shield ("Motion for Sanctions"). Dkt. 176. On October 28, 2021, the Honorable Susan Illston referred this Motion for Sanctions to the undersigned. Dkt. 193.

Plaintiffs seek these terminating sanctions under Federal Rule of Civil Procedure 37(b), 37(c), 37(e), and the Court's inherent power in response to OnlineNIC and ID Shield's consistent, continuous and extensive spoliation of evidence. Having carefully considered the Parties' submissions and oral arguments, and for the reasons discussed below, the Court **GRANTS AS MODIFIED** Plaintiffs' Motion for Sanctions.

I. BACKGROUND

A. Factual Allegations – the Parties

Plaintiffs Facebook and Instagram, known globally for their free online social networking services, own numerous trademarks and service marks, including the word marks FACEBOOK

and INSTAGRAM. Dkt. 109 (Second Amended Complaint ("SAC")) at ¶¶ 18–24. Plaintiffs have registered these marks with the United States Patent and Trademark Office ("Plaintiffs' Marks") and have continuously used their respective marks in interstate commerce in the United States in connection with their online networking services—Facebook, since 2004 and Instagram, since 2010. SAC at ¶¶ 19–25.

Defendant OnlineNIC is a domain name registrar accredited by ICANN[1] that sells, registers, and transfers domain names for third parties. SAC ¶ 9, 26. As relevant here, a domain name registrar processes domain name registration applications and submits such information to a central registry. Dkt. 201 at 3. The domain name registrar is responsible for maintaining the registration information (e.g., the applicant's name and contact information). *Id.* Some of this registration information is publicly available in the WHOIS directory.[2] *Id.*

OnlineNIC controls the operations of Defendant ID Shield. SAC ¶ 33. ID Shield registers the requested domain names of OnlineNIC's customers so that ID Shield appears as the registrant in the WHOIS directory rather than the customer. SAC ¶ 27. ID Shield then allegedly licenses the domain names back to OnlineNIC's customers. SAC ¶ 10. Put more simply, ID Shield enables OnlineNIC's customers to own domain names anonymously.

B. Factual Allegations – the Claims

Plaintiffs bring four claims against all defendants: (1) cybersquatting under the Anti-Cybersquatting Consumer Protection Act ("ACPA"); (2) trademark infringement; (3) false designation of origin; and (4) dilution. SAC ¶¶ 76–137. These claims principally arise out of defendants' alleged registration of and trafficking in 35 domain names that are identical to or confusingly similar to Plaintiffs' Marks (the "Infringing Domain Names"). SAC ¶ 56. The Infringing Domain Names include domains that seek to take advantage of users' typos in entering a domain (e.g., www-facebook-login.com) or a desire to artificially inflate one's online presence (e.g., buyinstagramfans.com). *Id.* ID Shield is listed as the registrant in the WHOIS directory for

[1] The Internet Corporation for Assigned Names and Numbers ("ICANN") accredits domain name registrars to register internet domain names.
[2] The WHOIS directory contains information identifying the owners of a domain name. *See* Dkt. 109-7.

each of the Infringing Domain Names. SAC ¶ 57. Plaintiffs allege that some of the Infringing Domain Names have been used for malicious activities, including phishing and selling tools for hacking. SAC ¶ 67.

Plaintiffs claim that their authorized representatives sent five or more notices to ID Shield with evidence that the Infringing Domain Names had harmed Plaintiffs. SAC ¶ 74. Under OnlineNIC's Registration Agreement, Plaintiffs contend ID Shield is required to disclose contact information for its customers within seven days of receipt of "reasonable evidence of actual harm" or else it must accept liability. SAC ¶ 71; Ex. 4 to SAC. Plaintiffs further claim that ID Shield failed to timely disclose its customers' contact information following receipt of Plaintiffs' notices regarding the Infringing Domain Names. SAC ¶ 75. This action resulted.

C. Procedural History

This case has a long history before this Court prior to its reassignment to Judge Illston on September 28, 2021. Dkt. 173. Plaintiffs filed suit on October 28, 2019 [Dkt. 1] and served their initial document requests on March 20, 2020 [Dkt. 176 at 4]. OnlineNIC and ID Shield served tardy discovery responses and made an initial production of documents on June 9, 2020. Dkt. 58 at 2-3. Owing to issues with the manner of production, including the absence of Bates numbers and requested metadata, OnlineNic and ID Shield re-produced these documents on July 23, 2020. Dkt. 176 at 13. Persisting issues with the production and allegations of data dumping resulted in motion practice and a hearing before this Court on November 10, 2020. Dkt. 53. Following three subsequent productions[3] of their ticket database, discussed *infra*, on February 10, 2021, the Parties filed a joint discovery letter brief and supplemental briefs. Dkt. 62; Dkt. 64; Dkt. 65.

In the joint discovery letter brief, Plaintiffs argued that without the appointment of a special discovery master, Defendants OnlineNIC and ID Shield's conduct would prevent Plaintiffs from obtaining accurate and complete evidence of Defendants OnlineNIC and ID Shield's conduct regarding the native database records. Dkt. 62 at 1. This Court held a hearing on February 16, 2021, and on March 3, 2021, appointed Thomas Howe Special Discovery Master ("Special

[3] OnlineNIC and ID Shield produced documents on December 26, 2020; February 4, 2021; and February 5, 2021. Dkt. 115 at 10.

Master") to determine both the adequacy of Defendants OnlineNIC and ID Shield's past productions and whether they destroyed or withheld data from their ticket database. Dkt. Nos. 66, 72.

On March 24, 2021, this Court granted Plaintiffs' motion for leave to file a First Amended Complaint ("FAC") to add Defendant Xiamen 35.com Internet Technology Co., Ltd. ("35.CN"). Dkt. 81. Plaintiffs filed their FAC on March 31, 2021. Dkt. 84. On April 16, 2021, Defendants OnlineNIC and ID Shield filed their answer to the FAC. Dkt. 88. On June 1, 2021, this Court granted the Parties' stipulation to file a Second Amended Complaint ("SAC"), which Plaintiffs filed on the same day. Dkt. 108; Dkt. 109. The Court granted the Parties' stipulation to deem Defendants OnlineNIC and ID Shield's Answer to the FAC as their operative responsive pleading to the SAC. Dkt. 108.

The Special Master completed his review and filed his report on July 12, 2021. Dkt. 115 ("Special Master's Report" or "SMR"). On July 20, 2021, Plaintiffs and Defendants OnlineNIC and ID Shield filed statements of non-opposition to the Special Master's Report. Dkt. 125; Dkt. 126. On August 10, 2021, this Court adopted the findings of the Special Master. Dkt. 151.[4] Accordingly, the key findings, now findings of the Court, are set forth below.

D. Special Master's Data Destroyed or Withheld Report

As stated above, this Court appointed the Special Master on March 3, 2021, and charged him with (1) supervising and completing Defendants' collection, search, and production to Plaintiffs' counsel of the ticket database; (2) producing a result set of responsive data to the parties in native database format; and (3) determining whether data was destroyed or withheld from the ticket database. Dkt. 72. Defendants' Kayako Ticket Database ("Ticket Database"), the subject of the spoliation concerns, comprised communications between OnlineNIC and ID Shield and their customers. Dkt. 219 at 13:22–24, 21:17–19, 22:23–25.[5] It also contained records of attachments

[4] OnlineNIC and ID Shield never withdrew or sought to withdraw their statement of *Non-opposition to Special Master's Report* (Dkt. 126). Nor have Defendants received special permission to challenge the conclusions in the Special Master's Report, the deadline for challenging it having long since passed.

[5] OnlineNIC and ID Shield also produced a "Registration Database," which allegedly contained "millions of transactional records about their registration business, including customer contact

to those communications, though the attachments themselves were stored in the file system on the server (outside the database). SMR at 26. These attachments included copyright notifications, email conversations, legal demands, account summaries, complaints, letters, legal information, and financial information. *Id.* Plaintiffs allege that notices of cybersquatting from other trademark owners—including, presumably, the notices Plaintiffs claim to have sent regarding their own marks—would have been included in those attachments. Dkt. 176 at 5.

To perform his analysis, the Special Master reviewed OnlineNIC and ID Shield's previous productions to Plaintiffs and collected data directly from Defendants. SMR at 5. In total, the Special Master collected 184 GB of Electronically Stored Information ("ESI") data comprising 545,013 files and 442,680,623 database records. SMR at 2. After more than three months of extensive review and collection efforts, including five status reports [Dkt. Nos. 83, 86, 89, 105, and 112], the Special Master filed his Data Destroyed or Withheld Report, in which he concluded that there is "ample evidence that Defendants failed to preserve responsive ESI, deleted ESI, and withheld ESI." SMR at 2. He found that Defendants deleted over one half (52.35%) of the ticket-related database records and that 30% of those records—approximately 3,317,816 records—were responsive to the original discovery protocol. *Id.* at 2–3. In light of the second, more expansive discovery protocol, the Special Master estimates that the number of responsive records deleted and forever lost to Plaintiffs would be higher. *Id.*

1. OnlineNIC and ID Shield Failed to Preserve ESI.

The Special Master found that OnlineNIC and ID Shield "failed to preserve potentially relevant ESI for this matter pre-litigation, post complaint filing, during discovery, and even after the appointment of Special Master." SMR at 17. In reviewing the evidence, the Special Master theorized two possibilities regarding Defendants' backup management systems: (1) Defendants were remiss, and the backup management system was wholly inadequate or (2) the backup management system was actually robust, and Defendants had concealed their data backups from

information, customer credit cards and bank information." Dkt. 47 at 1; Dkt. 48 at ¶ 5. At the hearing, Plaintiffs' counsel explained that notices of cybersquatting would not have been included in the Registration Database. Dkt. 219 at 23:14–20.

the Special Master. SMR at 18–19.

The Special Master found that despite selling backup services to their clients and demonstrating advanced software skills, OnlineNIC and ID Shield had not implemented comprehensive backup systems by the filing of the complaint on October 28, 2019. SMR at 18. Nor had they implemented even basic backup management software by the time the Special Master was appointed more than a year later on March 3, 2021. SMR at 18.

OnlineNIC and ID Shield also lied about their backup management system and generally obfuscated their backup processes. SMR at 19. They claimed in discovery that backups did not exist, but the Special Master discovered evidence of backups on two servers in multiple locations. *Id.* Moreover, the Special Master determined that some of OnlineNIC and ID Shield's prior productions to Plaintiffs would have required creating backups for the data. *Id.* Those backups were neither produced nor disclosed. *Id.*

The Special Master opined that "it is likely there are additional files, including developer script files, on undisclosed or unlocated developer workstations or servers." SMR at 19, 30.

2. OnlineNIC and ID Shield Actively Deleted Records Before and After the Special Master's Appointment.

OnlineNIC and ID Shield deleted 2,919,130 records from the Ticket Database between May 16, 2013, and December 16, 2020, indicating that Defendants still were actively deleting evidence more than a year after this action was filed on October 28, 2019. SMR at 23. Between December 16, 2020, and March 23, 2021, the Special Master found that a further 4,102,283 records were "deleted and missing" in the live Ticket Database. *Id.* By the time of his final collection of attachment files on March 23, 2021, he also found that Defendants had deleted 331,390 of 432,033 attachment files from the file system. SMR at 26.

Defendants deleted database records in the live Ticket Database ***after*** this litigation had commenced and ***after*** initially producing those records to Plaintiffs: "During multiple productions from Defendants, some records were contained in one production but were missing from subsequent productions and from the live Ticket Database itself." *Id.* The Special Master identified at least three instances in which the version of the Ticket Database he received

contained fewer records than the productions Plaintiffs had received earlier in the suit. SMR at 22–23. He also found that "Defendants deleted SQL files and databases they previously provided Plaintiffs" given that two databases produced to Plaintiffs between December 2020 and February 2021 are no longer located on Defendants' servers or workstations. SMR at 28. OnlineNIC and ID Shield do not dispute that they deleted records. SMR at 37.

The Special Master further determined that OnlineNIC and ID Shield had deleted tickets and related ticket posts from the live Ticket Database *after that data was initially produced to him*. *Id.* at 23, 27. On March 12, 2021, Defendants produced a backup of the live Ticket Database to the Special Master. SMR at 27. By comparing the records in the backup Ticket Database from March 12, 2021 to the live Ticket Database, the Special Master found that Defendants deleted more than 1,000 tickets from the live Database after those records initially were produced to him in the backup Ticket Database. SMR at 27. The Special Master requested that Defendants produce 251 matching HTML files located on the Kayako Ticket Server that had not been included in the prior productions. *Id.* Defendants provided these files on April 26, 2021. *Id.* The Special Master found that the code used to produce the HTML files was not located on the servers, evidencing that "Defendants deleted records from the Ticket database during discovery." *Id.* at 28. Based on the prefixes used for the HTML files, the Special Master concluded that "there were most likely other files with prefix names for other search terms that were deleted or removed after they were created on March 12, 2021 and were not available for subsequent productions." *Id.*

Similarly, by comparing a text file created on March 17, 2021 to directory lists from servers and developer workstations as they existed on or after April 26, 2021, the Special Master found evidence that Defendants had deleted 472 physical attachment files after March 17, 2021. SMR at 29. That same text file showed the existence of undisclosed servers. *Id.* at 30.

Defendants also created at least 28 PHP scripts and 1 SQL script specifically designed to delete database records and attachment files. SMR at 28–29. Scripts are essentially tools that can be used to produce and delete database records. *Id.* at 28. This evidence forced the Special Master's conclusion that Defendants programmatically deleted files using these scripts and then attempted to hide their activities by deleting the scripts as well. *Id.* at 29.

3. OnlineNIC and ID Shield Concealed Evidence from Plaintiffs and the Special Master.

OnlineNIC and ID Shield consistently withheld records from Plaintiffs. The Parties' initial discovery protocol included a date filter of July 1, 2015 to July 14, 2020. SMR at 30; *see also* Exhibit 2 to SMR. However, the Special Master found that Defendants used different date ranges when culling data for past productions to Plaintiff and consequently withheld two years' worth of ESI. SMR at 30. Defendants also withheld ESI as a result of their inconsistent execution of search terms when they made their prior productions to Plaintiffs. SMR at 31. More egregiously, Defendants failed to apply the search terms to the full text of ticket attachment files—the files likely to contain infringement notices—to determine responsiveness: "All these attachments subsequently were not produced, and some were in fact deleted. . . ." *Id.* Of the ticket attachment files OnlineNIC and ID Shield did produce, the attachments either were "missing file extensions," which prevented Plaintiffs from opening them, or "contained virus files." SMR at 32–33. Finally, the Special Master found that Defendants engaged in data dumping by producing to Plaintiffs 27,823,240 records when only 5,096 of those records were responsive. SMR at 35.

OnlineNIC and ID Shield also repeatedly misled the Special Master or failed to cooperate with him. The Special Master had to make multiple requests of Defendants for files and information before Defendants complied, and on some occasions, failed to respond altogether. In one instance, they claimed that no programming files existed on their servers and then included such files in a production to the Special Master on April 26, 2021. SMR at 19. In another instance, they failed to provide or disclose the existence of an entire database to the Special Master. *Id.* The Special Master asked Defendants to provide all database files and backup files, but many of the requested files Defendants ultimately produced were "omitted or incomplete." SMR at 33. Defendants also deleted a file that was a Ticket Database backup. SMR at 33. Initially following the Special Master's request for the file, Defendants claimed the file did not exist. "When questioned further, Defendants claimed they deleted this file to free up space on their server on April 11, 2021 . . . ." *Id.* No backup of the "directly responsive, relatively small" file was kept, and a server directory list Defendants produced on June 7, 2021 at the Special

Master's request confirmed that the file was no longer on the server. *Id.* at 34.

Although the Special Master was able to recover some of the deleted records, he concluded that Defendants' conduct caused Plaintiffs "irreparable harm" and further that Plaintiffs would "continue to suffer harm" because of Defendants' mass spoliation of evidence. SMR at 40.

E. Plaintiffs' Motion to Strike Defendants OnlineNIC and ID Shield's Answer and for Default Judgment.

After receiving the Special Master's Report, Plaintiffs filed a motion to strike Defendants' answer and for default judgment against Defendants OnlineNIC and ID Shield. Dkt. 117. Defendants OnlineNIC and ID Shield filed a statement of non-opposition to this motion. Dkt. 120. On July 21, 2021, Plaintiffs filed an emergency *ex parte* application for a temporary restraining order freezing Defendants OnlineNIC and ID Shield's assets. Dkt. 129. Defendants OnlineNIC and ID Shield partially opposed the *ex parte* application. Dkt. 131. This Court granted in part and denied in part Plaintiffs' *ex parte* application and set a hearing for the preliminary injunction. Dkt. 132. Plaintiffs and Defendants OnlineNIC and ID Shield then filed a stipulation concerning Defendants' payments owed to Special Master and the conversion of the temporary restraining order into a preliminary injunction with revised terms. Dkt. 141. The Court granted the stipulation and vacated the preliminary injunction hearing. Dkt. 143; Dkt. 144. On August 3, 2021, Plaintiffs filed a statement confirming the Special Master's balances were paid in full. Dkt. 148.

On August 10, 2021, this Court held a status conference to discuss (1) the formal adoption of the Special Master's Report; (2) the status of the preliminary injunction; (3) the pending motion for default judgment; and (4) defense counsel's pending motion to withdraw as counsel. Dkt. 150; Dkt. 153. On August 16, 2021, Plaintiffs filed a statement that they do not intend to seek to sever or dismiss Defendant Xiamen 35.com Internet Technology Co. ("35.CN") from this action. Dkt. 155. On September 22, 2021, 35.CN declined magistrate judge jurisdiction and the case was reassigned to Judge Illston. Dkt. 168; Dkt. 173.

After reassignment, Plaintiffs renoticed the instant Motion before Judge Illston. Dkt. 176. Defendant 35.CN filed an opposition to Plaintiffs' Motion for Sanctions [Dkt. 183], and

Defendants OnlineNIC and ID Shield moved to withdraw their earlier statement of non-opposition. Dkt. 185. On October 28, 2021, Judge Illston referred the Motion for Sanctions to the undersigned. Dkt. 193. The Court issued an order on November 2, 2021, granting Defendant 35.CN's motion to file an opposition and setting a briefing schedule for Defendants OnlineNIC and ID Shield's opposition and Plaintiffs' reply. Dkt. 198. Defendants OnlineNIC and ID Shield filed their opposition on November 23, 2021, and Plaintiffs filed their reply on December 10, 2021. Dkt. 201; Dkt. 206. The matter came on for hearing before the undersigned on March 1, 2022.

II. LEGAL STANDARD

"When a district court decides to impose sanctions or discipline, it must clearly delineate under which authority it acts to insure that the attendant requirements are met." *Williams v. Williams*, No. 07-4464, 2013 WL 3157910, at *4 (N.D. Cal. June 20, 2013) (citing *Weissman v. Quail Lodge, Inc.*, 179 F.3d 1194, 1200 (9th Cir. 1999)). Federal courts have the power to sanction litigants for discovery misconduct under both the Federal Rules of Civil Procedure and the court's inherent power to prevent abusive litigation practices. *Leon v. IDX Sys. Corp.*, 464 F.3d 951, 958 (9th Cir. 2006).

Facebook and Instagram seek terminating sanctions under four sources of authority: Federal Rule of Civil Procedure 37(e) ("Rule 37(e)"), Federal Rule of Civil Procedure 37(b) ("Rule 37(b)"), Federal Rule of Civil Procedure 37(c) ("Rule 37(c)"), and the Court's inherent authority to sanction. Because the Court will issue terminating sanctions under Rule 37(e), Rule 37(b), and Rule 37(c), it need not consider whether it may also sanction OnlineNIC and ID Shield under its inherent power.

Defendants contend, and Plaintiffs do not dispute, that a preponderance of the evidence standard should apply for terminating sanctions. Dkt. 176 at 7 n.6; Dkt. 201 at 2; *see also WeRide Corp. v. Kun Huang*, No. 18-7233-EJD, 2020 WL 1967209, at *9 (N.D. Cal. Apr. 16, 2020) (concluding that a preponderance of the evidence standard applies on a motion for terminating sanctions) (Davila, J.).

III. ANALYSIS

A. Terminating Sanctions Are Warranted under Rule 37(e).

Rule 37(e) permits sanctions when a party fails to preserve ESI. In evaluating whether spoliation of ESI has occurred, courts should consider whether: "(1) the ESI 'should have been preserved in the anticipation or conduct of litigation'; (2) the ESI 'is lost because a party failed to take reasonable steps to preserve it'; and (3) '[the ESI] cannot be restored or replaced through additional discovery.'" *Porter v. City of San Francisco*, No. 16-3771, 2018 WL 4215602, at *3 (N.D. Cal. Sept. 5, 2018) (quoting Rule 37(e)). Where these three criteria are met and the Court finds that the "party acted with the intent to deprive another party of the information's use in the litigation," a court may issue terminating sanctions. Fed. R. Civ. Proc. 37(e)(2)(C). Although Rule 37(e) does not define "intent," courts have found that "intent" in this context means "the evidence shows, or it is reasonable to infer, that a party purposefully destroyed evidence to avoid its litigation obligations." *Phan v. Costco Wholesale Corp.*, No. 19-5713, 2020 WL 5074349, at *2 (N.D. Cal. Aug. 24, 2020); *see also First Fin. Sec., Inc. v. Freedom Equity Grp., LLC*, No. 15-1893, 2016 WL 5870218, at *3 (N.D. Cal. Oct. 7, 2016) (finding evidence of intent where defendants' agents deleted text messages and formed "explicit agreement to avoid communicating electronically," suggesting an intent to prevent discovery of incriminating facts). "[T]here is no requirement that the court find prejudice to the non-spoliating party under Rule 37(e)(2)." *Porter*, 2018 WL 4215602, at *3.

The Court finds that the criteria are easily satisfied here and that spoliation has occurred. The duty to preserve arises when litigation is pending or reasonably foreseeable. *First Fin. Sec., Inc.*, 2016 WL 5870218, at *3. At the latest, OnlineNIC and ID Shield were on notice of a duty to preserve ESI upon being served with the original Complaint on November 11, 2019. Dkt. 15. However, by the time of the Special Master's appointment more than a year later, Defendants either had failed to implement a basic backup management system or had concealed their backup databases. SMR at 18-19. Moreover, OnlineNIC is no stranger to litigation. OnlineNIC has appeared before this Court three times since 2008, each time represented by the same counsel who represents it in this action. *See Verizon Cal. Inc. v. Onlinenic, Inc.*, No. 08-2832, 2009 WL

2706393 (N.D. Cal. Aug. 25, 2009); *Yahoo! Inc. v. Onlinenic Inc.*, No. 08-5698 (N.D. Cal.); *Microsoft Corp. v. OnlineNIC Inc.*, No. 08-4648 (N.D. Cal.).[6] OnlineNIC and ID Shield are technologically sophisticated parties that, by now, should be well-acquainted with their preservation obligations under Rule 37(e). SMR at 17-18. There is simply no excuse for their failure to preserve ESI.

Here, the second criterion – that the party failed to take reasonable steps to preserve the ESI – is also met. Fed. R. Civ. Proc. 37(e); *WeRide Corp.*, 2020 WL 1967209, at *12. Defendants admit to deleting vast amounts of ESI after the filing of the Complaint, during discovery, and after the Special Master's appointment. SMR at 37; Dkt. 202 ("Freeman Declaration") at ¶ 5 ("OnlineNIC does not dispute that certain database records were deleted from the production Kayako Database after the complaint in this case was filed on October 28, 2019[.]"). Indeed, the evidence demonstrates that Defendants redoubled their efforts to delete data after this suit was filed: whereas Defendants deleted 2,919,130 database records between May 16, 2013 and December 16, 2020, they deleted 4,102,283 database records between December 16, 2020 and March 23, 2021. SMR at 23.

Defendants argue that their mass deletions and general obfuscation of their data and ESI make it impossible for the Special Master to conclude that the spoliation occurred after the filing of the Complaint. Dkt. 201 ("Opposition") at 2, 5. This argument is without merit. First, OnlineNIC readily admitted that it deleted data after the Complaint was filed. Freeman Declaration ¶ 5. Second, the Special Master found conclusive evidence that Defendants deleted database records between productions to Plaintiffs and after productions to the Special Master. SMR at 22. In one instance, the Special Master found that Defendants had deleted more than 1,000 tickets from the live Database after those records initially were produced to him in the backup Ticket Database. SMR at 27.

The third requirement is that the ESI cannot be restored or replaced through additional discovery. Fed. R. Civ. Proc. 37(e). Although the Special Master was able to recover some of the

[6] The Court takes judicial notices of these cases pursuant to Fed. R. of Evid. 201.

withheld and deleted records, "other responsive ESI will be unavailable because the data was destroyed and no longer exists." SMR at 40. Of particular note, Defendants deleted 76.7% of the attachments – 331,390 of 432,033 attachment files – which comprised copyright notifications, legal demands, account summaries, complaints, and legal information. SMR at 40. The Special Master estimated 77,247 of the attachment files would have been responsive. SMR at 27. Plaintiffs claim that the deleted attachments "all speak to the number, timing, and nature of any notices or other legal complaints received by Defendants concerning cybersquatting" and "potentially would have shown a pattern of bad faith intent to profit by Defendants and their customers." Dkt. 176 at 10. Further, under the second, more expansive discovery protocol, "[d]ue to Defendants' data destruction efforts, the new production will be inadequate because it will not include all responsive ESI that should have been produced to Plaintiffs." SMR at 40-41. This Court previously has determined that where recovery of ESI is minimal and the spoliation vast, the third factor is satisfied. *WeRide Corp.*, 2020 WL 1967209, at *12. Such is the case here.

Before a court may issue sanctions under Rule 37(e)(2), it must find that "the party acted with the intent to deprive another party of the information's use in the litigation." Here, the Special Master concluded that the mass spoliation of evidence was "consistent," "continuous," and "intentional" and that Plaintiffs suffered "irreparable harm." SMR at 26, 39–40. "Deletion activities were so pervasive that they included many database tables . . . and attachment files. Of the deleted records, Special Master estimates 30% of those records . . . or 3,317,816 were responsive to the agreed past discovery protocol." SMR at 39. As the Court has adopted the Special Master's Report, the Court finds that Defendants intentionally sought to avoid producing responsive documents and other ESI to Plaintiffs. Dkt. 151. The Court notes that Defendants' intent is also clearly evidenced by their deliberate disobedience of the Court's March 3, 2021 order appointing the Special Master. Despite the Court's clear instructions to grant the Special Master unencumbered access to the Ticket Database and any backup copies, Defendants withheld ESI, failed to disclose databases, and deleted backup files. *See John v. County of Lake*, No. 18-6935, 2020 WL 3630391, at *7 (N.D. Cal. July 3, 2020) ("Intent cannot be clearer when the District Court gave such an explicit, detailed explanation of Defendants' obligations and when Defendants

blatantly defied that specific order.").

The 2015 Advisory Committee Note to Rule 37(e) cautions that "the severe measures authorized by [37(e)(2)] should not be used when the information lost was relatively unimportant or lesser measures such as those specified in subdivision (e)(1) would be sufficient to redress the loss." Plaintiffs claim that the ESI lost was "crucial" to their case [Dkt. 176 at 9] because such records might have evidenced that Defendants intended to profit from the Infringing Domain Names and that Defendants knew that the Infringing Domain Names were being used for malicious activities [Dkt. 206 at 6-7]. As noted above, the Special Master found that Defendants deleted or withheld 76.7% of the ticket attachments, which comprised the "most critical" type of evidence. SMR at 40. Defendants' behavior made it impossible for the Special Master to determine how much of the non-recoverable ESI was responsive, but in his estimation, Defendants irreparably harmed Plaintiffs. *Id.* In light of the overwhelming evidence cited above, the Court agrees with Plaintiffs that the deleted or withheld ESI likely could have been probative of their claims.

As a lesser sanction, OnlineNIC and ID Shield propose "a jury instruction that reverses the onus of proof" such that Defendants would bear the burden of proving that they did not register, traffic in, or use the Infringing Domain Names. Dkt. 201 at 2.[7] This proposal in no way cures the harm to Plaintiffs because evidence that Defendants *did* register, traffic in, or use the Infringing Domain Names has been withheld or deleted. In other words, a shifting of the burden of proof does not improve Plaintiffs' lot, as they would be "equally helpless to rebut" Defendants' evidence at trial as they are now. *Leon*, 464 F.3d at 960; *WeRide Corp.*, 2020 WL 1967209 at *11. The Court finds that no jury instruction, monetary sanction, or exclusion of evidence will right the wrong occasioned by OnlineNIC and ID Shield's extensive spoliation. Accordingly, based on the facts articulated by the Special Master and adopted by this Court, the Court deems it appropriate to issue terminating sanctions under Rule 37(e).

[7] At the hearing, Defendants proposed a stipulation as well, discussed at III(B)(5), *infra*.

B. Terminating Sanctions Are Warranted under Rule 37(b)(2)(A)(vi).

Under Rule 37(b), a court may strike pleadings in whole or in part or enter default judgment where a party "fails to obey an order to provide or permit discovery, including an order under Rule 26(f), 35, or 37(a)[.]" Fed. R. Civ. Proc. 37(b)(2)(A). Before imposing terminating sanctions, the court must weigh the following factors: "(1) the public's interest in expeditious resolution of litigation; (2) the court's need to manage its docket; (3) the risk of prejudice to the party seeking sanctions; (4) the public policy favoring disposition of cases on their merits; and (5) the availability of less drastic sanctions." *Leon*, 464 F.3d at 958 (quoting *Anheuser-Busch, Inc. v. Natural Beverage Dist.*, 69 F.3d 337, 348 (9th Cir. 1995)). Courts should not apply these factors mechanically; the factors supply a framework to guide the Court's decision. *Conn. Gen. Life Ins. Co. v. New Images of Beverly Hills*, 482 F.3d 1091, 1096 (9th Cir. 2007). Although the Court is not required to make explicit findings as to each factor, a finding of "willfulness, fault, or bad faith" is required for dismissal to be proper. *Leon*, 464 F.3d at 958. Rather, "the most critical factor is not merely delay or docket management concerns, but truth," and the Court's chief concern therefore should be "whether the discovery violations 'threaten to interfere with the rightful decision of the case.'" *Conn. Gen. Life Ins. Co.*, 482 F.3d at 1097 (internal citation omitted). Additionally, "[d]ue process concerns further require that there exist a relationship between the sanctioned party's misconduct and the matters in controversy such that the transgression 'threaten[s] to interfere with the rightful decision of the case.'" *Anheuser-Busch*, 69 F.3d at 348.

In its March 3, 2021 order appointing the Special Master, the Court ordered OnlineNIC and ID Shield to provide the Special Master "unencumbered access to their entire Support Ticket Database, any backup copies of the Support Ticket Database, and any third-party vendor hosting or storing the Support Ticket Database or any backup copies for Defendants." Dkt. 72 at 2. The Court further ordered Defendants to "provide the Special Master all passwords, encryption keys, database owner logins, licenses, credentials and database connection strings to transfer or access the database files and login to the Support Ticket Database and backups." *Id.* Neither Plaintiffs nor Defendants dispute that this order is one "to provide or permit discovery" within the meaning

of Rule 37(b). *See also Williams*, 2013 WL 3157910, at *4.

1. OnlineNIC and ID Shield Acted Willfully and in Bad Faith.

A party's spoliation of evidence qualifies as willful when the party has "some notice that the documents were potentially relevant to the litigation before they were destroyed." *Leon*, 464 F.3d at 959. Bad faith is demonstrated by "delaying or disrupting the litigation or hampering enforcement of a court order." *Id.* at 961 (internal citations omitted). OnlineNIC and ID Shield's conduct demonstrates both willfulness and bad faith.

First, Defendants behaved willfully by withholding and destroying evidence after Plaintiffs filed their initial Complaint [Dkt. 1], First Amended Complaint [Dkt. 84], and Second Amended Complaint [Dkt. 109], all of which put Defendants on notice of the nature of Plaintiffs' claims. These pleadings, together with the discovery requests Plaintiffs propounded and the first discovery protocol to which the parties agreed, clearly set forth the relevant time period and domain names at issue. And yet, Defendants intentionally deleted over 11 million database records, more than 4 million of which were deleted after this litigation had been underway for a year. SMR at 23, 39. Defendants accomplished this mass deletion, in part, by creating 29 scripts specifically designed to delete database records. SMR at 28. More than 3 million of the deleted records likely would have been responsive to the past discovery protocol. *Id.* at 39. Defendants also withheld and deleted ticket attachments, which, as discussed above, were likely to contain the most responsive ESI. *Id.* The intentional and systematic deletion of potentially discoverable evidence over the years that this case has been pending in this Court, and particularly during the Special Master's review, clearly demonstrates willfulness. *See, e.g.*, *Leon*, 464 F.3d at 959 (affirming district court's finding of willful spoliation where plaintiff was aware of duty to preserve data "but intentionally deleted many files and then wrote a program to write over deleted documents"); *WeRide*, 2020 WL 1967209, at *10 (finding willfulness where defendant "left in place the autodelete settings on its email server, began using DingTalk's ephemeral messaging feature, and maintained a policy of wiping the computers of former employees").

Second, in addition to Defendants' widespread deletion activities, which alone evidence bad faith, OnlineNIC and ID Shield have proceeded in bad faith throughout most of this litigation.

Defendants failed to cooperate with the Special Master, deleted files after producing them to Plaintiffs and to the Special Master, concealed documents from the Special Master, applied the wrong filters when conducting reviews of potentially discoverable material and consequently withheld years' worth of ESI, engaged in data dumping, and produced documents to Plaintiffs that were missing file extensions or contained viruses. Defendants' behavior toward the Special Master clearly hampered enforcement of this Court's discovery order because the Special Master's report could not be produced until July 2021. Accordingly, the Court finds that Defendants acted in bad faith.

2. The First, Second, and Fourth Factors

The first factor, "the public's interest in expeditious resolution of litigation" and the second factor, "the court's need to manage its dockets" generally favor terminating sanctions. *Computer Task Grp. Inc. v. Brotby*, 364 F.3d 1112, 1115 (9th Cir. 2004). Such is the case here, where OnlineNIC and ID Shield's misconduct, detailed above, has delayed resolution of this matter. The fourth factor – "public policy favoring disposition of cases on their merits" – usually cuts against sanctions. *Id.* Defendants argue that this case deserves to be heard on the merits because they have produced a "mountain" of exculpatory evidence. Dkt. 201 at 6–7. In particular, they highlight examples of emails OnlineNIC sent Facebook and Instagram in response to their complaints regarding some of the Infringing Domain Names and alleged issues with the Special Master's analysis. *Id.*; Freeman Declaration ¶ 15, Ex. A. At the hearing, Defendants argued that such exculpatory evidence supports deciding this case on the merits. Dkt. 219 at 6:21–24; 8:19–9:6. Defendant 35.CN, against which no motion for sanctions is pending, also sought to underscore the "unique legal issue" of imputed liability to a domain name registrar resulting from the ICANN agreement that is present in this case. *Id.* at 18:5–12. The Court finds that the fourth factor weighs against sanctions because, as Defendants correctly note, public policy favors resolution of cases on the merits. However, for the reasons set forth below, the Court holds that the remaining factors weigh heavily in favor of sanctions.

3. The Third Factor

The risk of prejudice to the party seeking sanctions is the most important factor for case

dispositive sanctions because it "looks to whether the [spoliating party's] actions impaired the [non-spoliating party's] ability to go to trial or threatened to interfere with the rightful decision of the case." *Leon*, 464 F.3d at 959. Courts in the Ninth Circuit have found prejudice where another party's failure to produce documents forced the non-spoliating party to "rely on incomplete and spotty evidence," *Anheuser-Busch*, 69 F.3d at 354; where the plaintiff engaged in a mass deletion of 2,200 files from his work computer during litigation, *Leon*, 464 F.3d at 959–60; and where a defendant engaged in mass destruction of emails and email accounts, *WeRide*, 2020 WL 1967209, at *10–11.

Here, Defendants join the same company of bad actors. Both the case law and the record in this case amply support a finding of prejudice. As set forth above, the Special Master found that Plaintiffs have suffered "irreparable harm" and will "continue to suffer harm" because of Defendant's spoliation of evidence. SMR at 39–40. Massive amounts of ESI, including the critical attachment files, are "not recoverable" and therefore "lost forever" to Plaintiffs. SMR at 4. OnlineNIC and ID Shield argue that "plaintiffs never tie what was allegedly spoliated with the Infringing Domain Names." Dkt. 201 at 5. As a preliminary matter, Plaintiffs obviously do not know the details of what was spoliated: "a record that cannot be seen, cannot be searched." SMR at 40. "Any moving party is at a disadvantage to show prejudice because a moving party who seeks evidence cannot prove that relevant evidence existed but was destroyed." *John*, 2020 WL 3630391 at *7 (finding in context of Rule 37(e)(1) that defense counsel's and defendants' lies about defendants' use of their cell phones to communicate about work provided "an even stronger inference" that there were other relevant text messages that Defendants had spoliated)[8]; *see also Apple, Inc. v. Samsung Elecs. Co. Ltd.*, 888 F. Supp. 2d 976, 993 (N.D. Cal. 2012) ("[T]hough neither Apple nor the Court may ever know the contents of any destroyed Samsung emails, the fact that the emails of key Samsung witnesses were among those destroyed permits the reasonable inference that Apple was prejudiced by Samsung's spoliation.").

That being said, the Special Master's Report details the *types* of records and attachments

[8] Although *John* discussed prejudice in the context of Rule 37(e)(1), the discussion applies with equal force under Rule 37(b).

deleted and further estimates the percentage of records that would have been responsive to the initial discovery protocol. It is impossible to know how many documents would have been responsive. However, the ticket attachments, which comprised, *inter alia*, email conversations, legal demands, and account summaries, likely would have featured prominently in Plaintiffs' prosecution of their case. For example, in the SAC, Plaintiffs allege that OnlineNIC and ID Shield registered the Infringing Domain Names to divert consumers from the authentic websites for commercial gain. SAC ¶ 86. Email conversations between Defendants and their clients regarding the Infringing Domain Names could have revealed the clients' purpose in registering the Infringing Domain Names or Defendants' knowledge of the purpose to which the Infringing Domain Names were being put.

OnlineNIC and ID Shield claim they have mountains of exculpatory evidence, yet for all Plaintiffs or the Court may ever know, those "mountains" may be dwarfed by the mountains of damning evidence Defendants deleted. The Court finds that Plaintiffs have been prejudiced.

4. The Fifth Factor

The final factor, the availability of less drastic sanctions, calls upon the Court to consider (1) "the feasibility of less drastic sanctions" and explain why alternative sanctions would be inappropriate; (2) whether it "implemented alternative sanctions before ordering dismissal," and (3) whether the Court issued a warning of the possibility of dismissal. *Leon*, 464 F.3d at 960.

The Court already has considered the feasibility of the lesser sanction OnlineNIC and ID Shield proposed in their moving papers and has found it insufficient to address the harm done to Plaintiffs. *See supra*, III(A). At the hearing, Defendants proposed, in addition to shifting the burden of proof, that they would stipulate to a bad faith intent to profit if Plaintiffs proved the other elements of cybersquatting. Dkt. 219 at 44:9–19. Under 15 U.S.C. § 1125(d)(1)(A)(i), a person is liable for cybersquatting if, as relevant here, that person (1) has a bad faith intent to profit from the mark; and (2) registers, traffics in, or uses a domain name that is identical or confusingly similar to a distinctive mark or is identical, confusingly similar to, or dilutive of a famous mark. Thus, Defendants' stipulation would relieve Plaintiffs of proving one of the key elements of their claims.

The Court finds that this augmented proposal is still insufficient. Although generous on its face, it does not mitigate the issue with the initial proposal: even if it is Defendants' burden to prove that they did *not* register, traffic in, or use the Infringing Domain Names, Defendants have spoliated vast amounts of ESI and documents that might have proved that they *did* engage in cybersquatting with respect to the Infringing Domain Names. Plaintiffs have no way of rebutting Defendants' evidence.

When faced with incidents of mass spoliation, the Ninth Circuit and this Court have found that "any jury instruction or exclusion of evidence would be inappropriate." *WeRide*, 2020 WL 1967209, at *11; *Leon*, 464 F.3d at 960 (affirming dismissal where the district court found that less drastic sanctions would be useless because a ruling excluding evidence would be "futile," and a jury instruction would still leave Defendants unable to rebut Plaintiffs' evidence); *Anheuser-Busch*, 69 F.3d at 352 (affirming dismissal sanction where defendants' "pattern of deception and discovery abuse made it impossible for the district court to conduct another trial with any reasonable assurance that the truth would be available"). Here, OnlineNIC and ID Shield have lied to Plaintiffs and the Special Master, destroyed evidence before and after this case began, and impeded resolution of this case by failing to make complete and timely productions to Plaintiffs and the Special Master. The Court is sensitive to the drastic nature of a terminating sanction but finds that any lesser sanction would be inappropriate under the circumstances.

As to the second factor, this Court issued an order appointing the Special Master to supervise discovery and exhorting OnlineNIC and ID Shield to provide the Special Master unencumbered access to the Ticket Database and any backup copies. Dkt. 72. Defendants did not comply with this order.

Finally, the third factor is partially inapplicable because OnlineNIC and ID Shield destroyed some of the ESI before litigation began and before the Court had any opportunity to warn them against such destruction. *See WeRide*, 2020 WL 1967209 at *11; *Leon*, 464 F.3d at 960. After litigation had commenced, the undersigned issued multiple orders concerning Defendants' conduct in discovery. *E.g.*, Dkt. 54 (ordering Defendants to de-designate and de-duplicate their production); Dkt. 60 (granting stipulated extension given substantial outstanding

discovery disputes regarding Defendants' production); Dkt. 66 (ordering parties to prepare proposed order for appointment of special master). Here, the Court did not expressly warn Defendants of the possibility of terminating sanctions for violating its order. However, by the time the Court appointed the Special Master at the latest, Defendants were on notice that their discovery abuses were of grave concern. Express warnings are not always necessary, and a party "can hardly be surprised by a harsh sanction in response to a willful violation of a pretrial order." *Malone v. U.S. Postal Serv.*, 833 F.2d 128, 133 (9th Cir. 1987).

In sum, considering that four of the five factors set forth in *Leon* weigh in favor of dismissal, the Court will issue terminating sanctions under Rule 37(b).

C. Terminating Sanctions Are Warranted under Rule 37(c)(1)(C).

Rule 37(c)(1) authorizes sanctions for failure to produce information under Rules 26(a) or 26(e). Federal Rule of Civil Procedure 26(e)(1) provides that parties that have made disclosures under Rule 26(a) or have responded to discovery requests or interrogatories, have an ongoing duty to supplement or correct their disclosure or response "(A) in a timely manner if the party learns that in some material respect the disclosure or response is incomplete or incorrect, and if the additional or corrective information has not otherwise been made known to the other parties during the discovery process or in writing. . . ." If a party fails in this duty to supplement, and the failure was not "substantially justified" or "harmless," Rule 37(c) authorizes a court, "on motion and after giving an opportunity to be heard" to "impose other appropriate sanctions, including any of the orders listed in Rule 37(b)(2)(a)(i)–(vi)." Fed. R. Civ. Proc. 37(c)(1)(C). Plaintiffs seeks default judgment against OnlineNIC and ID Shield, as permitted under Rule 37(b)(2)(a)(vi).

Courts have "particularly wide latitude" to issue sanctions under Rule 37(c)(1). *Yeti by Molly, Ltd. v. Deckers Outdoor Corp.*, 259 F.3d 1101, 1106 (9th Cir. 2001). Unlike Rule 37(b), it is not necessary for the Court to find that a violation of a court order has occurred because Rule 37(c)(1) is self-executing. *Id.* "[T]he rule is automatic in the sense that a district court *may* properly impose an exclusion sanction where a noncompliant party has failed to show that the discovery violation was either substantially justified or harmless." *Merchant v. Corizon Health, Inc.*, 993 F.3d 733, 740 (9th Cir. 2021) (emphasis in original). Accordingly, "[t]he party facing

sanctions bears the burden of proving that its failure to disclose the required information was substantially justified or is harmless." *R&R Sails, Inc. v. Ins. Co. of Penn.*, 673 F.3d 1240, 1246 (9th Cir. 2012).

Here, Plaintiffs point to the following misconduct in support of their motion under Rule 37(c)(1)(C): (1) throughout discovery, Defendants intentionally withheld responsive documents from Plaintiffs; (2) Defendants applied the incorrect search parameters, resulting in the withholding of records from Plaintiffs; (3) Defendants failed to disclose relevant servers; and (4) Defendants failed to produce files or records related to one of Defendants' customers. Dkt. 176 at 17. In short, Defendants' spoliation frustrated Plaintiffs' efforts to prove their case because the productions they received were incomplete and could not be fully supplemented as a result of the mass spoliation. Dkt. 176 at 4.

The Court now turns to Plaintiffs' request for terminating sanctions pursuant to Rule 37(c)(1)(C). Law in the Ninth Circuit appears unsettled as to whether a Court must address the same considerations at issue under Rule 37(b) when assessing terminating sanctions under Rule 37(c). Some courts apply the five factors set forth in *Leon*. *See, e.g.*, *Medtronic Vascular, Inc. v. Abbott Cardiovascular Sys., Inc.*, No. 06-1066, 2009 WL 2058245, at *1 (N.D. Cal. July 13, 2009) (citing *Wendt v. Host Int'l, Inc.*, 125 F.3d 806, 814 (9th Cir. 1997)); *Thompson v. Housing Authority of City of Los Angeles*, 782 F.2d 829, 831 (9th Cir. 1986) (analyzing the five factors where dismissal sanction issued for violation of pretrial orders). More recently, the Ninth Circuit formulated a two-factor test for courts to apply as part of the "harmlessness" inquiry where the exclusion of evidence under Rule 37(c)(1) amounts to dismissal of a claim: (1) the presence of willfulness, fault, or bad faith; and (2) the availability of lesser sanctions. *R & R Sails*, 673 F.3d at 1247. Although it is unclear if this test applies where terminating sanctions are sought, the Ninth Circuit has clarified that *R&R Sails* "did nothing to disturb Rule 37(c)(1)'s textual requirement that a party facing sanctions under that provision bears the burden of showing that a sanction other than exclusion is better suited to the circumstances." *Merchant*, 993 F.3d at 741. To meet that burden, the non-compliant party must specifically move for a lesser sanction; merely presenting arguments in opposition to a motion will not suffice. *Id.* at 741–42 ("Likewise, if the

noncompliant party fails to move for lesser sanctions, the district court is not required to consider one and does not abuse its discretion in excluding evidence where such action is otherwise justified.").

Here, the Court need not reach the issue of whether to apply the five-factor test in *Leon* or the two-factor test in *R&R Sails* because Defendants stumbled at the first step: they failed to file an independent motion for lesser sanctions. *See Merchant*, 993 F.3d at 741–42. Indeed, OnlineNIC and ID Shield's Opposition wholly fails to address Plaintiffs' arguments under Rule 37(c). *See* Dkt. 201. As such, Defendants have not carried their burden of proving that their failure to disclose was "substantially justified" or "harmless." Fed. R. Civ. Proc. 37(c)(1)(C). Moreover, the Court notes that even if it is required to apply the full five factors set forth in *Leon*, the Court's decision would be the same, as the Court already has evaluated those factors in detail above and would adopt that same analysis here. Accordingly, in the context of the Court's findings under Rule 37(e) and Rule 37(b), the Court also finds it appropriate to issue terminating sanctions under Rule 37(c) and will enter default judgment against OnlineNIC and ID Shield.[9]

IV. RELIEF

Having found it appropriate to issue terminating sanctions, the Court now addresses the array of remedies that Plaintiffs request. Specifically, Plaintiffs seek: (1) $3.5 million in statutory damages under the Anti-Cybersquatting Consumer Protection Act ("ACPA"); (2) injunctive relief; (3) attorneys' fees pursuant to 15 U.S.C. § 1117(a); and (4) reimbursement of costs associated with the Special Master. In assessing remedies, the Court takes the well-pleaded allegations of the SAC as true, except those relating to the amount of damages. *TeleVideo Sys., Inc. v. Heidenthal*, 826 F.2d 915, 917-18 (9th Cir. 1987); *Geddes v. United Fin. Grp.*, 559 F.2d 557, 560 (9th Cir. 1977). The Court considers each form of relief requested below.

A. Plaintiffs Are Entitled to Statutory Damages Under the ACPA.

The ACPA provides that a plaintiff may recover statutory damages pursuant to 15 U.S.C. § 1125(d)(1). Prevailing plaintiffs have the option of electing actual or statutory damages prior to

[9] Although the Court is entering default judgment against OnlineNIC and ID Shield, it declines to use Plaintiffs' proposed default judgment.

entry of final judgment. 15 U.S.C. § 1117(d). Here, Plaintiffs have elected to recover statutory damages, so the Court need not consider the measure for awarding actual damages. Dkt. 176 at 18. The Court has wide discretion to award statutory damages in an amount of "not less than $1,000 and not more than $100,000 per domain name, as the court considers just." 15 U.S.C. § 1117(d); *Verizon Cal. Inc.*, 2009 WL 2706393, at *3. Facebook and Instagram seek the maximum recovery for each of the 35 Infringing Domain Names identified in the SAC for a total of $3.5 million. SAC ¶ 56.

When determining an award of statutory damages, courts generally consider:

> the egregiousness or willfulness of the defendant's cybersquatting, the defendant's use of false contact information to conceal its infringing activities, the defendant's status as a 'serial' cybersquatter—i.e., one who has engaged in a pattern of registering and using a multitude of domain names that infringe the rights of other parties—and other behavior by the defendant evidencing an attitude of contempt toward the court or the proceedings.

Verizon Cal. Inc., 2009 WL 2706393, at *3; *see also* 15 U.S.C. § 1125(d)(1)(B)(i) (setting forth factors a court may consider in determining bad faith intent). Courts distinguish between instances of typosquatting, which takes advantage of consumers' common spelling errors, and cybersquatting, which includes the correct spelling of the plaintiff's trademarked name. *Facebook, Inc. v. Banana Ads LLC*, No. 11-3619, 2013 WL 1873289, at *16 (N.D. Cal. Apr. 30, 2013) (hereinafter, "*Banana Ads*").

1. Defendants' Conduct Was Egregious.

The Court first notes that OnlineNIC and ID Shield registered a significant number (35) of domain names (the Infringing Domain Names) incorporating both the correct spellings and misspellings of Plaintiffs' Marks. SAC ¶ 56. "The more infringing domain names a defendant registered or acquired, the more malicious the conduct." *Banana Ads*, 2013 WL 1873289, at *16 (awarding Facebook $1,340,000 for 47 infringing domain names registered by one defendant). Of the 35 Infringing Domain Names, the Court has identified 25 that use the correct spelling of Plaintiffs' Marks' (Facebook and Instagram) and 10 that employ misspellings of Plaintiffs' Marks. *Id.* The Court agrees with Plaintiffs that the Infringing Domain Names, such as "faecbook-page.com" and "iiinstagram.com," are identical or confusingly similar to Plaintiffs' legitimate

marks. Some of the Infringing Domain Names—e.g., "m-facebook-login.com"—also appear to have been used for malicious activity, "including hosting websites directing visitors to other commercial sites, phishing, and selling purported tools for hacking." SAC ¶ 67; Ex. 8 to SAC. Other of the Infringing Domain Names, like "facebook-mails.com," were used "in connection with email services, which is usually an indication that the domain name was used for phishing or other scams." SAC ¶ 68. Defendants clearly registered the Infringing Domain Names in an intent to profit from consumers' mistakes or confusion when trying to reach Plaintiffs' legitimate sites. *See, e.g.*, *Verizon Cal. Inc.*, 2009 WL 2706393, at *3; *Shields v. Zuccarini*, 254 F.3d 476, 484 (3d Cir. 2001). The Court can conceive of no other use for registering a domain name like "instakram.com."

Plaintiffs further argue that this Court should find that Defendants' conduct was willful and egregious because Plaintiffs failed to identify the customers who registered the Infringing Domain Names upon the requests of Plaintiffs' representative. SAC ¶ 74. OnlineNIC and ID Shield dispute these contentions. Dkt. 201 at 7–8; Exs. A, B to Freeman Declaration. The Court need not resolve this factual dispute. Under 15 U.S.C. § 1117(e), the acts of concealment include knowingly providing "materially false contact information to a domain name registrar, domain name registry, or other domain name registration authority in registering, maintaining, or renewing a domain name used in connection with the violation." The SAC does not allege that Defendants provided materially false contact information to a domain name registrar: as alleged, Defendants are the owners and licensors of the Infringing Domain Names, and Defendants did provide their own contact information for each of the Infringing Domain Names. SAC ¶¶ 57, 59.[10] The Court declines Plaintiffs' invitation to find Defendants' business model automatically results in a finding of willfulness under 15 U.S.C. § 1117(e) at this time. Nevertheless, for the reasons set forth above, the Court concludes that Defendants' conduct was egregious.

2. Defendant OnlineNIC Is a Serial Cybersquatter.

"In determining the proper amount of statutory damages, courts also consider whether the

[10] Plaintiffs allege in the SAC that OnlineNIC has operated under aliases in the past but does not allege that it did so here. *See* SAC ¶ 65.

defendant has engaged in a pattern of registering and monetizing large numbers of domain names that infringe the rights of other parties." *Verizon Cal. Inc.*, 2009 WL 2706393, at *5. This Court is not writing on a blank slate with respect to OnlineNIC: OnlineNIC has appeared before this Court, represented by the same counsel, no less than three times on similar allegations of cybersquatting. In *Verizon Cal. Inc.*, Plaintiffs obtained a $33.15 million default judgment against OnlineNIC, or $50,000 for each of 663 domain names that were identical or confusingly similar to Verizon's marks. 2009 WL 2706393, at *1. When denying OnlineNIC's request to set aside the default judgment, U.S. District Court Judge Fogel found that OnlineNIC had registered an "extraordinary" 14,700 domain names that infringed twenty-six other famous marks. *Id.* at *5.

Although Plaintiffs have not presented evidence that OnlineNIC has engaged in cybersquatting with respect to other famous marks, the Court has taken judicial notice of this Court's prior cases involving OnlineNIC. The Court finds that in the context of this history, OnlineNIC is a serial cybersquatter, whose activities were not even deterred by a $33.15 million judgment against it.

3. Defendants Have Demonstrated Contempt of These Proceedings.

The Court already has set forth above, in great detail, the bases for the terminating sanctions against Defendants. It further notes that Defendants' willful spoliation of millions of database records and thousands of attachments warrants a substantial per-violation award.

4. The Court Awards Defendants $3,135,000 in Statutory Damages.

Plaintiffs cite a variety of cases from this district and other federal courts in support of the maximum damages award per domain name. Dkt. 176 at 18–19. Nevertheless, the Court is not convinced that $100,000 per domain name is appropriate in this circumstance. The Court finds the decisions of other courts in this district instructive. In *Banana Ads*, Magistrate Judge Westmore set forth various factors that informed her award of statutory damages, including "the number of domain names registered, whether there was an attempt to conceal the registrant's identity, whether the correct spelling of Plaintiff's trademark is contained in the infringing domain names, whether an individual is a serial cybersquatter, and whether internet traffic was redirected" to other landing pages. 2013 WL 1873289, at *15. These factors incorporate the ACPA's bad faith

criteria, 15 U.S.C. § 1125(d)(1)(B)(i), and other factors the Court deemed relevant. *Id.* Magistrate Judge Westmore also found it appropriate to consider whether domain names incorporate the correctly-spelled mark alongside other correctly-spelled common words. *Id.* at *16; *see also Verizon Cal., Inc.*, 2009 WL 2706393, at *3. Similarly in *Bittorrent, Inc. v. Bittorent Mktg GMBH*, No. 12-2525-BLF, 2014 WL 5773197, at *11 (N.D. Cal. Nov. 5, 2014) and *Twitch Interactive, Inc. v. Johnston*, No. 16-3404-BLF, 2019 WL 3387977, at *11 (N.D. Cal. July 26, 2019) U.S. District Court Judge Beth Freeman looked to the *Banana Ads* framework in assessing statutory damages. This Court, likewise, finds that *Banana Ads* offers useful guidance.

At the hearing, in response to questions from the Court regarding determination of statutory damages Plaintiffs argued that the minimum amount of damages that should be awarded is $50,000 per domain name, the amount Judge Fogel awarded Plaintiffs for each domain name in *Verizon Cal. Inc.* Dkt. 219 at 33:17–24. Plaintiffs also distinguished *Banana Ads* on the grounds that *Banana Ads* did not involve a staggering degree of spoliation. *Id.* at 34:3–7. The Court finds these arguments persuasive. Further, a substantial statutory damages award should further the ACPA's "goal of deterrence." *Verizon Cal. Inc.*, 2009 WL 2706393, at *9.

The Court finds it appropriate to distinguish between instances of typosquatting and true cybersquatting on famous marks. *Banana Ads*, 2013 WL 1873289, at *16; *see also Verizon Cal. Inc.*, 2009 WL 2706393, at *3. The Court finds that domains containing the correctly-spelled "Facebook" and "Instagram" marks are more malicious than those misspelling the marks. *See Banana Ads*, 2013 WL 1873289, at *16; *Bittorrent, Inc.*, 2014 WL 5773197, at *12. As noted above, 10 of the 35 Infringing Domain Names involve typosquatting: (1) face2bouk.com; (2) facebux2.com; (3) facekhook.com; (4) facessbook.com; (5) faecb00k-page.com; (6) faecbook-page.com; (7) instaface.org; (8) instakram.com; (9) login-1nstargram.com; and (10) singin-1nstargram.com. SAC ¶ 56. The Court finds that a base award of $70,000 is appropriate for each of these domain names, and because OnlineNIC is a serial cybersquatter, assesses an additional $10,000 per offending domain name. Thus, Plaintiffs are entitled to an award of $80,000 per domain name that incorporates a confusingly similar misspelling of Plaintiffs' Marks.

"Registering a domain name by incorporating the correctly-spelled infringing mark with

other correctly-spelled common words is evidence of malicious conduct." *Twitch Interactive, Inc.*, 2019 WL 3387977, at *11. Here, 21 of the 35 Infringing Domain Names include correct spellings of Plaintiffs' Marks and correct spellings of other common words—e.g., "buyinstagramfans.com" and "www-facebook-pages.com." These domain names are particularly likely to deceive users who may be attempting to find various webpages on Plaintiffs' legitimate websites. The Court finds that a base of $70,000 per domain name is again appropriate and augments that amount by $25,000, the sum of $10,000 because OnlineNIC is a serial cybersquatter, $10,000 for additional evidence of malicious conduct, and $5,000 for identical spellings of Plaintiffs' Marks. In total, Plaintiffs are entitled to an award of $95,000 for each of these 21 domain names.

Finally, four of the 35 Infringing Domain Names incorporate identical spellings of Plaintiffs' Marks but do not include other commonly-spelled words: (1) facebook-alkamazasok.net; (2) iiinstagram.com; (3) facebook-pw.com; and (4) www-instagram.net. SAC ¶ 56. A base award of $70,000 per domain is appropriate with an enhancement of $15,000, the sum of $10,000 for OnlineNIC's status as a serial cybersquatter and $5,000 for identical spellings of Plaintiffs' Marks. Thus, Plaintiffs are awarded $85,000 for each of these four domain names.

Based on the foregoing, the Court concludes that Plaintiffs should be awarded $3,135,000 in damages, constituting $80,000 for each of 10 domain names that incorporate confusingly similar misspellings of Plaintiffs' Marks, $95,000 for each of 21 domain names that incorporate an exact spelling of Plaintiffs' Marks and another commonly spelled word, and $85,000 for each of four domain names that incorporate an exact spelling of Plaintiffs' Marks.

B. Transfer of Offending Domain Names.

Plaintiffs also request that Defendants be ordered to transfer to Plaintiffs the Infringing Domain Names, as well as "all domain names under [Defendants'] control which are identical or confusingly similar to Plaintiffs' Marks." Dkt. 176 at 24; Dkt. 176-4 ("Proposed Default Judgment") at ¶ 104.[11] The ACPA permits the Court to transfer offending domain names to the

[11] In the Proposed Default Judgment, Plaintiffs additionally sought "the remaining domain names owned or controlled by Defendants ('Defendants' Domain Names') free and clear of any liens or encumbrances to Plaintiffs as stipulated by Plaintiffs and Defendants on July 27, 2021 (ECF No. 141)." Dkt. 176-4 at ¶ 92. At the hearing, Plaintiffs stipulated to the transfer being limited to the

mark owner. 15 U.S.C. § 1125(d)(1)(C). Accordingly, the Court will order that the 35 Infringing Domain Names identified in ¶ 56 of the SAC be transferred to Plaintiffs.

C. Plaintiffs Are Entitled to Injunctive Relief.

Injunctive relief is permitted under 15 U.S.C. § 1116(a) to prevent further incidents of cybersquatting. "Injunctive relief is the remedy of choice for trademark and unfair competition cases, since there is no adequate remedy at law for the injury caused by defendant's continuing infringement." *Century 21 Real Estate Corp. v. Sandlin*, 846 F.2d 1175, 1180 (9th Cir. 1988). Courts considering permanent injunctive relief are still bound to consider whether a plaintiff has demonstrated: "(1) that it has suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction." *eBay Inc. v. MercExchange, LLC*, 547 U.S. 388, 391 (2006).

Under 15 U.S.C. § 1116(a), a plaintiff is "entitled to a rebuttable presumption of irreparable harm" upon a finding of a violation of 15 U.S.C. § 1125(d). OnlineNIC and ID Shield have not presented any evidence in rebuttal. Accordingly, as the Court has found Defendants in violation of 15 U.S.C. § 1125(d), the Court finds that Plaintiffs have suffered an irreparable harm. Plaintiffs also have established that the harm to their reputation and goodwill cannot be remedied through monetary damages. Dkt. 176 at 23; SAC at ¶¶ 98, 107–108, 119–120, 131–132. The balance of hardships and the public interest also weigh in favor of equitable relief. Despite the opportunity to do so, Defendants have failed to identify any hardship they would suffer from being permanently enjoined against infringing Plaintiffs' Marks. *See, e.g., Twitch Interactive, Inc.*, 2019 WL 3387977, at *12; *Facebook, Inc. v. 9 Xiu Network (Shenzhen) Tech. Co., Ltd.*, No. 19-1167-AGT, 2021 WL 5707741, at *7 (N.D. Cal. Oct. 21, 2021) (Tse, M.J.), adopted 2021 WL 5707740 (N.D. Cal. Nov. 16, 2021) (Tigar, J.)) ("It is no hardship to cease intentionally infringing someone else's trademark rights.") (citation omitted). Finally, given that the public may have been

Infringing Domain Names set forth in the SAC. Dkt. 219 at 36:12–20.

deceived or harmed by the ACPA violations, and considering that at least one of the defendants is a serial cybersquatter that was previously undeterred by a substantial statutory damages award, the Court finds the public's interest would not be disserved by entering an injunction. *See, e.g.*, *Bittorent, Inc.*, 2014 WL 5773197, at *13; *Twitch Interactive, Inc.*, 2019 WL 3387977, at *12. Under the circumstances, permanent injunctive relief is appropriate.

The Court now turns to the scope of the permanent injunction. Injunctive relief should be "narrowly tailored" to remedy the specific harm a plaintiff has identified "rather than 'to enjoin all possible breaches of the law.'" *Price v. City of Stockton*, 390 F.3d 1105, 1117 (9th Cir. 2004) (quoting *Zepeda v. INS*, 753 F.2d 719, 728 n.1 (9th Cir. 1983)). It is a precise tool to fix a precise injury. Federal Rule of Civil Procedure 65(d) instructs courts to state the terms of the injunction specifically and to "describe in reasonable detail—and not by referring to the complaint or other document—the act or acts restrained or required." Fed. R. Civ. Proc. 65(d)(1)(B) – (C). And Federal Rule of Civil Procedure 54(c) provides that default judgments "must not differ in kind from, or exceed in amount, what is demanded in the pleadings."

In view of these standards, Plaintiffs' proposed default judgment is unquestionably overbroad in that it seeks to enjoin Defendants not only from infringing Plaintiffs' Marks, but also from Defendants' business activities altogether. *See* Dkt. 176-4 at ¶ 101. For example, Plaintiffs seek to enjoin Defendants from "continuing to provide domain name registration services to the Licensees." Dkt. 176-4 at ¶ 101(f). Plaintiffs also seek to prevent Defendants from "[t]ransferring or withdrawing any funds from any bank account." Dkt. 176-4 at ¶ 103(b). Injunctions are not vehicles for putting the other party out of business. Although at the hearing Plaintiffs' counsel stipulated to amendments to ¶ 101(f) and ¶ 104(e) of the Proposed Default Judgment that ameliorate some of the Court's concerns over scope, the proposed injunction is unworkable in its present state. Indeed, Paragraphs 102 and 103 appear to have no bearing on the current posture of the case. *See* Dkt. 176-4 at ¶¶ 102–103. Additionally, at the hearing, Defendants' counsel indicated that ¶ 104(f) may run afoul of the European Union's General Data Protection Regulation. Dkt. 219 at 42:21–43:6. The Parties, accordingly, are ordered to meet and confer regarding the language of the proposed injunction and to submit a joint proposal consistent with

this Order.

D. Plaintiffs Are Awarded Their Attorneys' Fees in an Amount to Be Determined.

Plaintiffs seek to recover their attorneys' fees of $2,057,782.17 pursuant to 15 U.S.C. § 1117(a). Dkt. 176 at 24; Dkt. 176-1 ("Steele Declaration"). As a preliminary matter, the Court notes that, having found that Defendants violated a court order under Rule 37(b)(2)(A), the Court "must order the disobedient party, the attorney advising that party, or both to pay the reasonable expenses, including attorney's fees, caused by the failure, unless the failure was substantially justified or other circumstances make an award of expenses unjust." Fed. R. Civ. Proc. 37(b)(2)(C). Because the Parties did not brief this alternative ground for relief, and because the Court finds that this is an exceptional case warranting attorneys' fees under the Lanham Act, the Court does not reach this issue.

Section 1117(a) provides that a court may award attorney fees to the prevailing party in "exceptional cases." In *Octane Fitness, LLC v. ICON Health & Fitness, Inc.*, the Supreme Court held that an "exceptional" case is:

> simply one that stands out from others with respect to the substantive strength of a party's litigating position (considering both the governing law and the facts of the case) or the unreasonable manner in which the case was litigated. District courts may determine whether a case is 'exceptional' in the case-by-case exercise of their discretion, considering the totality of the circumstances.

572 U.S. 545, 554 (2014). The Ninth Circuit has held that *Octane Fitness* has "altered the analysis of fee applications under the Lanham Act" and now requires district courts to examine the totality of the circumstances in determining whether a case is exceptional. *SunEarth, Inc. v. Sun Earth Solar Power Co., Ltd.*, 839 F.3d 1179, 1181 (9th Cir. 2016). Courts should consider the nonexclusive factors identified in *Octane Fitness* and *Fogerty v. Fantasy, Inc.*, 510 U.S. 517 (1994) and should apply a preponderance of the evidence standard. *Id.*

"Courts applying the *Octane Fitness* analysis commonly find that willful infringement, in conjunction with non-participation in litigation, makes a case 'exceptional.'" *Facebook, Inc.*, 2021 WL 5707741, at *8 (quoting *ADG Concerns, Inc. v. Tsalevich LLC*, No. 18-0818, 2018 WL

4241967, at *13 (N.D. Cal. Aug. 31, 2018) (collecting cases), adopted 2018 WL 6615139 (N.D. Cal. Nov. 1, 2018)). This Court already has found (1) that OnlineNIC and ID Shield engaged in significant litigation misconduct, derailing discovery by spoliating evidence after this litigation began and after the Special Master was appointed, and (2) that Defendants' cybersquatting was egregious. These facts make the case exceptional, and attorneys' fees are warranted. As an award of attorneys' fees is discretionary under Section 1117(a), the Court has determined that Plaintiffs are only entitled to a partial recovery of fees: Plaintiffs are awarded fees related to the proceedings before the Special Master and the Motion for Sanctions.

Turning to the amount of fees to be awarded, the Court finds that it cannot ascertain whether the attorneys' fees sought are for the tasks covered by this Order or whether they are reasonable. As noted at the hearing, the chart in the Steele Declaration supporting the sanctions motion is insufficiently detailed: Plaintiffs list fees for broad categories such as "Pleadings" and "Motions" without any further explanation. Steele Declaration ¶ 2. Therefore, the Court orders Plaintiffs to submit additional supporting documentation as to the categories for which fees are awarded, including: (1) a description of work performed, (2) identification of which attorneys performed which tasks, (3) the number of hours worked, and (4) the billing rate for each attorney. OnlineNIC and ID Shield will have the opportunity to review and respond to Plaintiffs' submission of attorneys' fees.

E. Defendants Shall Reimburse Plaintiffs for Costs Associated with the Special Master.

Plaintiffs are entitled to recover their costs under Rule 37(b)(C)(2) and, as the prevailing parties on their claims, under 15 U.S.C. § 1117(a). In the Court's March 3, 2021 order appointing the Special Master, the Court initially provided that "the parties will divide the costs and fees of the Special Master such that Plaintiffs pay half and Defendants pay the remaining half." Dkt. 72 at 3. This order was without prejudice to a reallocation of the Special Master's costs at a later date. *Id.*

In Plaintiffs' Motion for Sanctions, they request $88,937 as a reimbursement for their

payment of the Special Master's costs and stipulated to that amount at the hearing.[12] Dkt. 176 at 25; Dkt. 219 at 47:21–22. The Court agrees that it is appropriate for Defendants to bear the entirety of the costs related to the Special Master. As the Special Master's costs are well-documented in this case (Dkt Nos. 124–143, 148), the Court is satisfied that the amount requested is reasonable. Accordingly, the Court orders Defendants to reimburse Plaintiffs $88,937 for the costs associated with the Special Master.

V. CONCLUSION

For the reasons stated above, the Court orders as follows:

1. The Court strikes the answer of OnlineNIC and ID Shield (Dkt. 88).
2. The Court enters default judgment against OnlineNIC and ID Shield.
3. The Court orders OnlineNIC and ID Shield to pay Plaintiffs $3,135,000 in statutory damages.
4. The Court orders OnlineNIC and ID Shield to reimburse Plaintiffs in the amount of $88,937 for costs related to the Special Master.
5. Within **21 days** of the issuance of this Order, Plaintiffs shall supplement their request for attorneys' fees, as provided for herein, with documentation supporting the amount of fees requested. OnlineNIC and ID Shield shall have the opportunity to review Plaintiffs' request and file any response within **14 days** of Plaintiffs' filing of the supplemental documentation.
6. The Parties shall meet and confer regarding revisions to Plaintiffs' proposed permanent injunction and shall file a joint revision within **21 days** of this Order's issuance, consistent with this Order.

SO ORDERED.

Dated: March 25, 2022

SUSAN VAN KEULEN
United States Magistrate Judge

[12] Plaintiffs' Proposed Default Judgment sought a recovery of $112,312.50 for costs related to the Special Master. Dkt. 176-4 at ¶ 91.