

1 Bradley P. Hartman (#017263)
John D. Titus (#012912)
2 **HARTMAN TITUS PLC**
3507 N. Central Ave., Suite 101
3 Phoenix, AZ 85012-2121
Phone: (602) 235-0500
4 Email: bhartman@hartmantitus.com
jtitus@hartmantitus.com
5 *Attorneys for Plaintiffs*

6
7 **IN THE UNITED STATES DISTRICT COURT**
8 **FOR THE DISTRICT OF ARIZONA**

9
10 Proofpoint, Inc., a Delaware corporation,
11 and Wombat Security Technologies, Inc., a
12 Delaware corporation,

13 Plaintiffs,

14 vs.

15 Facebook, Inc., a Delaware corporation,
16 and Instagram, LLC, a Delaware limited
liability company,

17 Defendants.
18

Civil No. _____

**COMPLAINT FOR DECLARATORY
RELIEF UNDER THE LANHAM ACT**

19 This is a suit by Proofpoint, Inc., and Wombat Security Technologies, Inc.
20 (“Plaintiffs”), against Defendants, Facebook, Inc., and Instagram, LLC (“Defendants”), for
21 declaratory relief under the Lanham Act pursuant to 28 U.S.C. § 2201.
22

23 **INTRODUCTION**

24 1. This is an action for declaratory relief pursuant to 28 U.S.C. § 2201 to establish
25 that Plaintiffs’ registration and use of the internet domain names <facebook-login.com>,
26 <facebook-login.net>, <instagramn.ai>, <instagramn.net>, and <instagramn.org> (the “Domain
27
28



1 Names”) is not unlawful under the Anticybersquatting Consumer Protection Act, 15 U.S.C.
2 § 1125(d) (the “ACPA”), or otherwise under the Lanham Act, 15 U.S.C. § 1051 *et. seq.*

3 2. This action is also filed to prevent the transfer of the Domain Names to
4 Defendants, which was ordered in an administrative decision on January 25, 2021, under the
5 Uniform Domain Name Dispute Resolution Policy (the “UDRP”) in a non-binding
6 proceeding captioned *Facebook, Inc. and Instagram, LLC v. WhoisGuard Protected,*
7 *WhoisGuard, Inc. / Phishing Operations, Wombat Security Technologies, World Intellectual*
8 *Property Organization Arbitration and Mediation Center, Case No. D2020-3218.*

9 **PARTIES**

10 3. Plaintiff, Wombat Security Technologies, Inc., is a Delaware corporation.
11 Wombat Security Technologies, Inc., is owned and operated by Proofpoint, Inc., a Delaware
12 Corporation. Wombat Security Technologies, Inc., and Proofpoint, Inc., are collectively
13 referred to as “Proofpoint.” Proofpoint has offices at 925 West Maude Avenue, Sunnyvale,
14 CA 94085.

15 4. On information and belief, Defendant, Facebook, Inc., is a Delaware
16 corporation with a principal place of business at 1 Hacker Way, Menlo Park, California
17 94025.

18 5. On information and belief, Defendant, Instagram, LLC, is a Delaware limited
19 liability company with a principal place of business at 1601 Willow Road, Menlo Park,
20 California 94025.

21 **JURISDICTION AND VENUE**

22 6. This Court has subject matter jurisdiction over this action pursuant to Section
23 39 of the Trademark Act of 1946 (the “Lanham Act”), 15 U.S.C. § 1121, and under 28
24 U.S.C. §§ 1331 and 1338(a). More specifically, this Court has jurisdiction pursuant to 28
25 U.S.C. § 1331 because this cause arises under 15 U.S.C. § 1114 in that Plaintiffs are the
26 registrant of Domain Names that are subject to transfer under a policy provided by the
27 registrar thereof relating to alleged conflict with a trade or service mark claimed by
28

1 Defendants, and under 28 U.S.C. § 2201(a) “In a case of actual controversy within its
2 jurisdiction, . . . any court of the United States, upon the filing of an appropriate pleading,
3 may declare the rights and other legal relations of any interested party seeking such
4 declaration, whether or not further relief is or could be sought.”

5 7. This Court has personal jurisdiction over Defendants because Defendants
6 agreed to submit to the jurisdiction of this Court when they initiated an administrative
7 proceeding pursuant to the UDRP concerning the Domain Names. Specifically, Defendants
8 agreed in their UDRP complaint to “submit, with respect to any challenge that may be made
9 by the Respondent to a decision by the Administrative Panel to transfer or cancel the Domain
10 Names that are the subject of this Complaint, to the jurisdiction of the principal office of the
11 concerned Registrar.”

12 8. The registrar for the Domain Names is NameCheap, Inc., a Delaware
13 corporation with principal offices at 4600 East Washington Street, Suite 305, Phoenix,
14 Arizona 85034.

15 9. Venue is proper in this district pursuant to 28 U.S.C. § 1391(b), as a substantial
16 part of the events giving rise to the claims occurred in this district. Furthermore, the registrar
17 of the Domain Names is located in this district.

18 **FACTS**

19 10. Proofpoint is a leading, publicly traded enterprise security company with a
20 market capitalization of approximately \$7 billion. Proofpoint provides software as a service
21 and other products for inbound email security, outbound data loss prevention, social media,
22 mobile devices, digital risk, email encryption, electronic discovery (“eDiscovery”), and
23 email archiving.

24 11. Proofpoint’s solutions protect organizations’ greatest assets and biggest risks:
25 their people. Its cybersecurity solutions include the following:

- 26 a) preventing email and cloud-based threats, including malware, credential
27 phishing and email fraud;

- 1 b) reducing successful phishing attacks and malware by helping people
2 spot and report unsafe email and by safeguarding their personal digital
3 activity;
- 4 c) securing digital channels and blocking impostor attacks and malicious
5 content that use trusted and lookalike email and web domains, social
6 media, the dark web, and more;
- 7 d) protecting sensitive data and assisting with compliance with ever-
8 evolving regulations;
- 9 e) collecting, archiving, supervising and monitoring sensitive data in a
10 compliant and legally defensible manner; and
- 11 f) providing security awareness training, including phishing simulation
12 training campaigns, to customers to help train them on how to spot and
13 properly respond to phishing attacks.

12 12. Proofpoint has been widely recognized by third parties for its effective
13 cybersecurity solutions that have protected many companies from online deception. For
14 example, Forbes recently published an article based on an interview with Proofpoint's CFO,
15 Paul Auvil. *See* Exhibit A,
16 [https://www.forbes.com/sites/jeffthomson/2020/12/04/cybersecurity-in-an-age-of-financial-](https://www.forbes.com/sites/jeffthomson/2020/12/04/cybersecurity-in-an-age-of-financial-threats-a-qa-with-proofpoints-cfo/?sh=76dc8d5b19ed)
17 [threats-a-qa-with-proofpoints-cfo/?sh=76dc8d5b19ed](https://www.forbes.com/sites/jeffthomson/2020/12/04/cybersecurity-in-an-age-of-financial-threats-a-qa-with-proofpoints-cfo/?sh=76dc8d5b19ed). The online magazine Information
18 Age also recently published an article around Proofpoint's Senior Sales Director Rob Bolton
19 discussing cybersecurity threats in the work-from home-reality. *See* Exhibit B,
20 [https://www.information-age.com/proofpoint-gm-discusses-insider-threats-work-from-](https://www.information-age.com/proofpoint-gm-discusses-insider-threats-work-from-anywhere-reality-123492767/)
21 [anywhere-reality-123492767/](https://www.information-age.com/proofpoint-gm-discusses-insider-threats-work-from-anywhere-reality-123492767/). A sampling of Proofpoint's many awards and recognitions –
22 which are too numerous to detail here – may be found in Exhibit C,
23 <https://www.proofpoint.com/us/news?type=All#in-the-news>.

24 13. One of the ways Proofpoint provides its cybersecurity solution services is by
25 conducting training to help its clients' workforce recognize cybersecurity threats, including
26 phishing attacks.

27 14. To make the training exercise more realistic, Proofpoint uses intentionally
28 domain names that look like typo-squatted versions of recognizable domain names, such as

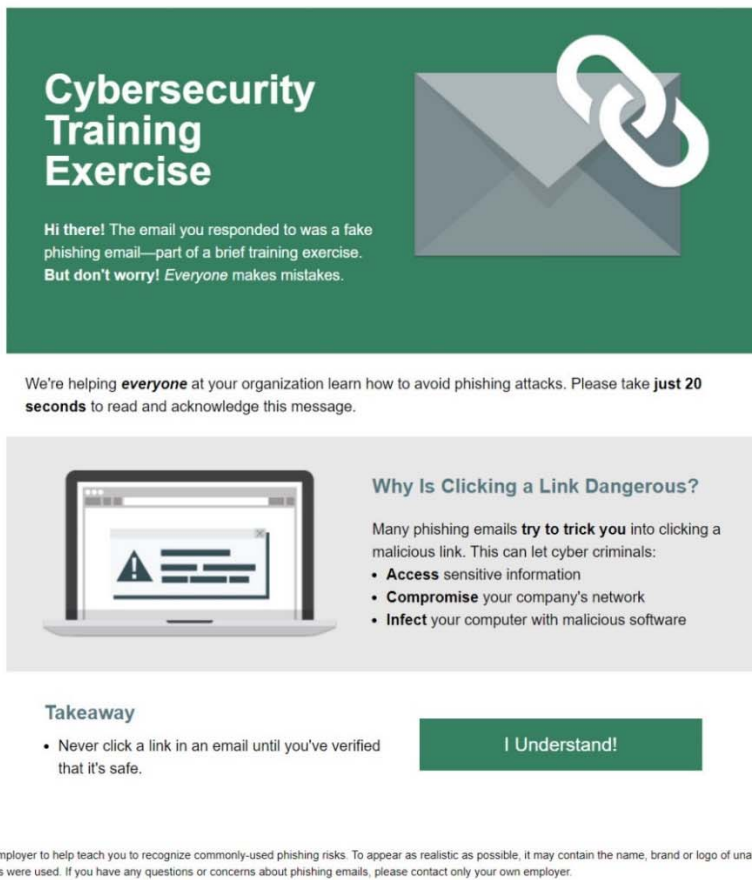
1 <facebook-login.com>, <instagarn.org> and the other Domain Names at issue in these
2 proceedings.

3 15. By using domain names similar to those of well-known companies, Proofpoint
4 is able to execute a more effective training program because the workforce is more likely to
5 learn to distinguish typo-squatted domains, which are commonly abused by bad actors to
6 trick workers, from legitimate domain names. This protects both the employer that provides
7 this training to its workforce as well as the owners of legitimate domain names, including
8 social-media companies like Defendants.

9 16. As part of its cybersecurity solution services, Proofpoint sends an imitation
10 phishing e-mail containing the Domain Names to people undergoing training. The
11 individuals undergoing training either (a) ignore the fake phishing email; (b) report the
12 email; or (c) click the simulated phishing link in the email, leading them to one of the
13 Domain Names, in which event they receive a teachable moment notice informing them that
14 they responded to a phishing attempt as part of a training exercise. This process helps to
15 reinforce the desired behavior of the recipient, which is to ignore or report the phishing email
16 attack, or to be taught the proper behavior in case the recipient did in fact click on the
17 simulated phishing link. A representative example of such a teachable moment notice is
18 shown below:

19
20
21
22
23
24
25
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



See Exhibit D.

17. Individuals who receive the imitation e-mail and click on the simulated phishing link are directed to a teachable moment notice, such as the one shown above. By doing so, Proofpoint is helping those individuals who were baited into clicking on the simulated phishing link to safely learn from their mistakes and further train them to identify similar malware, phishing, and Internet bad actors so that they can avoid actual cybersecurity breaches in the future.

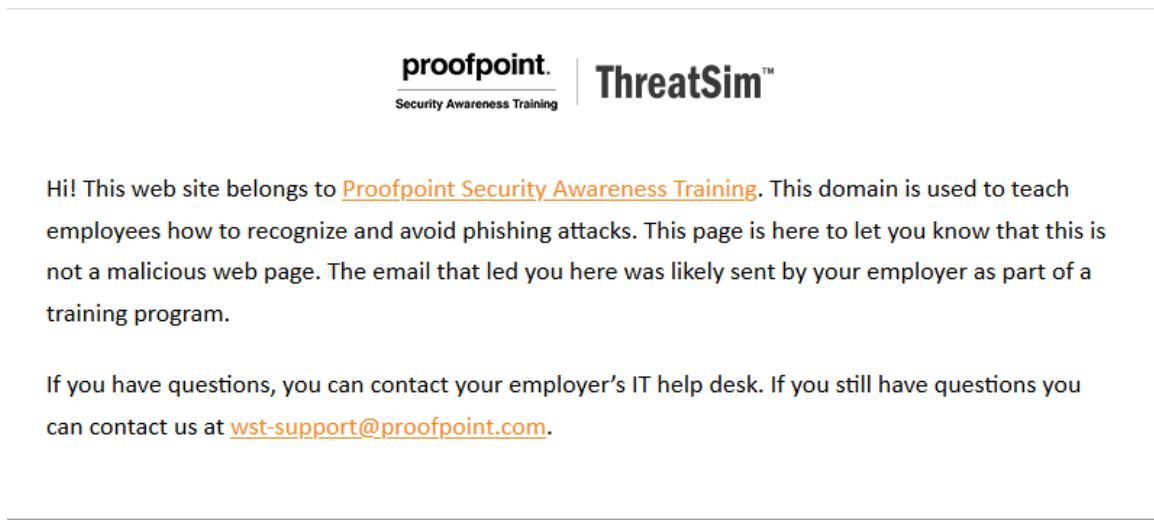
18. As shown in the image above, this representative teachable moment notice includes a disclaimer that states in part: “This phishing simulation was provided by your employer to help teach you to recognize commonly-used phishing risks. To appear as

1 realistic as possible, it may contain the name, brand or logo of *unaffiliated* third parties.”

2 Exhibit D (emphasis added).

3 19. Each teachable moment notice that is displayed when an individual clicks on
4 an simulated phishing link in Plaintiffs’ cybersecurity imitation emails includes a disclaimer
5 similar to the one shown in Exhibit D.

6 20. When consumers visit the Domain Names outside of Plaintiffs’ cybersecurity
7 imitation phishing emails, i.e., when consumers type in one of the Domain Names into an
8 internet address bar, that consumer is shown the following message:



18 See Exhibit E.

19 21. The message on the websites displayed at the Domain Names immediately
20 informs visitors that the domain *belongs* to Proofpoint and is being used for training services
21 *offered by Proofpoint*.

22 22. Proofpoint’s registration and use of the Domain Names has been in good faith
23 and for a legitimate purpose.

24 23. Proofpoint’s registration and use of the Domain Names also is a fair use of the
25 relevant trademarks of Defendants.

26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UDRP Proceeding

24. On or about November 30, 2020, Defendants filed a UDRP action against Plaintiffs alleging the Domain Names are confusingly similar to Defendants’ trademarks FACEBOOK and INSTAGRAM.

25. In the UDRP proceeding, Defendants alleged Proofpoint is not making use of the Domain Names in connection with a *bona fide* offering of goods or services.

26. In fact, Plaintiffs do have legitimate interests in using the Domain Names in connection with the *bona fide* offering of services to the public.

27. Plaintiffs have made legitimate fair use of the Domain Names, and such use does not suggest an association between Plaintiffs and Defendants or create a reasonable likelihood of consumer confusion regarding the source of Plaintiffs’ services or the source of Defendants’ services.

28. Consumer confusion is unlikely because Proofpoint clearly states on the websites to which the Domain Names are pointed: “Hi! This web site belongs to Proofpoint Security Awareness Training. This domain is used to teach employees how to recognize and avoid phishing attacks.” *See* Exhibit E.

29. Thus, consumers who reach the Domain Names by typing the Domain Names into an internet address bar know that the domain belongs to Proofpoint and that any services related to the domains originate from Proofpoint and not from Defendants.

30. Customer confusion also is unlikely among those individuals participating in Plaintiffs’ cybersecurity training programs because the teachable moment notice displayed when individuals click the link for one of the Domain Names includes a disclaimer similar to the following: “This phishing simulation was provided by your employer to help teach you to recognize commonly-used phishing risks. To appear as realistic as possible, it may contain the name, brand or logo of unaffiliated third parties.” *See* Exhibit D.

31. In the UDRP proceeding, Defendants alleged Proofpoint registered and used the Domain Names in bad faith.

1 32. In fact, Plaintiffs registered and used the Domain Names in good faith as part
2 of their business of providing effective training programs that enable employees to learn to
3 distinguish typo-squatted domains from legitimate domain names.

4 33. Registration of the Domain Names by Plaintiffs was lawful.

5 34. Notwithstanding Plaintiffs’ lawful registration and use of the Domain Names,
6 on January 25, 2021, an arbitrator appointed by the World Intellectual Property Organization
7 Arbitration and Mediation Center issued a decision ordering transfer of the Domain Names
8 to Defendants.

9 35. On January 27, 2021, the World Intellectual Property Organization Arbitration
10 and Mediation Center notified Namecheap of the UDRP decision ordering transfer of the
11 Domain Names to Defendants.

12 36. Under the UDRP, Namecheap will transfer the Domain Names to Defendants
13 within ten business days of receiving notification of the UDRP decision unless legal action
14 for independent determination of the Plaintiffs’ rights is commenced by Plaintiffs in this
15 judicial district.

16 **COUNT I**

17 **Declaratory Relief – Non-Violation of the Lanham Act under 28 U.S.C. § 2201**

18 37. Plaintiffs re-allege paragraphs 1 through 36 as if fully set forth herein.

19 38. Plaintiffs’ registration and/or use of the Domain Names does not violate
20 Defendants’ rights under the Lanham Act.

21 39. In registering the Domain Names, Plaintiffs did not have “bad faith intent,” as
22 provided in 15 U.S.C. § 1125(d)(1)(A)(i), to profit from Defendants’ alleged trademark
23 rights.

24 40. At the time Plaintiffs registered the Domain Names and at all times subsequent
25 thereto, Plaintiffs have used, and have intended to use, the Domain Names for legitimate or
26 fair-use purposes.

27
28

1 41. Plaintiffs had reasonable grounds to believe that their registration and/or use of
2 the Domain Names was a fair use or otherwise lawful use, as provided in 15 U.S.C.
3 § 1125(d)(1)(B)(ii).

4 42. Plaintiffs reasonably believe their registration and use of the Domain Names
5 was and is lawful under the Lanham Act.

6 43. There is an actual controversy with respect to whether the Defendants are
7 entitled to obtain transfer of the Domain Names away from Plaintiffs based on Defendants'
8 alleged rights under the Lanham Act.

9 44. In the absence of a declaration from the Court, Namecheap will transfer the
10 Domain Names to the control of Defendants, and Plaintiffs will suffer immediate and
11 irreparable harm.

12 45. Such real and actual controversy is of sufficient immediacy and reality to
13 warrant declaratory relief.

14 46. Plaintiffs' registration and use of the Domain Names does not, and is not likely
15 to, cause confusion, or to cause mistake, or to deceive as to the affiliation, connection or
16 association of Plaintiffs with Defendants, or as to the origin, sponsorship, or approval of
17 Plaintiffs' services or commercial activities by Defendants.

18 47. Plaintiffs' registration and use of the Domain Names do not misrepresent the
19 nature, characteristics, qualities, or geographic origin of Plaintiffs' services or Defendants'
20 goods, services, or commercial activities.

21 48. Plaintiffs seek a judicial declaration pursuant to 28 U.S.C. § 2201 that
22 (a) Plaintiffs' registration of the Domain Names was not in bad faith, (b) Plaintiffs' use of
23 the Domain Names will not cause confusion or mistake or deceive the public, and (c) by
24 registering and using the Domain Names, Plaintiffs have not infringed, and do not infringe,
25 any valid trademark rights of Defendants.

1 **DEMAND FOR TRIAL BY JURY**

2 49. Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiffs
3 hereby demand a trial by jury on any issue so triable.

4 **PRAYER FOR RELIEF**

5 WHEREFORE, Plaintiffs request judgment against the Defendants as follows:

- 6 A. A declaration by the Court, pursuant to 28 U.S.C. § 2201, that Plaintiffs’
7 registration, ownership and use of the Domain Names <facebook-login.com>,
8 <facebook-login.net>, <instagramn.ai>, <instagramn.net>, and <instagramn.org>
9 are lawful and proper and do not infringe any right the Defendants may claim;
10 B. A declaration by the Court, pursuant to 15 U.S.C. § 1114(D)(2)(v), that the
11 registration of the Domain Names is not unlawful under the ACPA or
12 otherwise under the Lanham Act, and the Domain Names are to be unlocked
13 and reactivated with full ownership and use restored to Plaintiffs; and
14 C. Awarding such other and further relief as the Court deems just and proper.
15

16 DATED this 9th day of February, 2021.

17 **HARTMAN TITUS PLC**

18 By: /s/ Bradley P. Hartman

19 _____
20 Bradley P. Hartman
21 John D. Titus
22 3507 N. Central Ave., Suite 101
23 Phoenix, Arizona 85012-2121

24 **PATTISHALL McAULIFFE NEWBURY
25 HILLIARD & GERALDSON, LLP**

26 200 South Wacker Drive, Suite 2900
27 Chicago, Illinois 60606

28 *Attorneys for Plaintiffs*