

0300
GEGHAMPÁI ÁFKÍ ÁÚT
SÖÖÁUWÞVÝ
ÚWÚÖÜQÜÁÖUWÜVÁÖŠÖÜS
ÖÖÖÖ
ÖÖÜÖÁKÖGÖFÖHÖHÖÖÖ

IN THE SUPERIOR COURT OF THE STATE OF WASHINGTON
FOR THE COUNTY OF KING

HOLD SECURITY LLC, a Wisconsin
Limited Liability Company

Plaintiff,

vs.

MICROSOFT CORPORATION, a
Washington Corporation,

Defendant.

No. _____

COMPLAINT

Plaintiff Hold Security (“Plaintiff” and/or “Hold Security”) alleges as follows:

I. PARTIES

1.1 Plaintiff Hold Security LLC (“Hold”) is a Wisconsin Limited Liability Company with its principal place of business in Mequon, Ozaukee County, Wisconsin.

1.2 Defendant Microsoft Corporation (“Microsoft”) is a Washington Corporation with its principal place of business in Redmond, King County, Washington.

II. JURISDICTION AND VENUE

2.1 This Court has subject matter jurisdiction pursuant to RCW 2.08.010.

2.2 Microsoft is subject to personal jurisdiction in this Court pursuant to RCW

COMPLAINT - 1

SCHWABE, WILLIAMSON & WYATT, P.C.
Attorneys at Law
1420 5th Avenue, Suite 3400
Seattle, WA 98101-4010
Telephone: 206-622-1711

1 4.28.185.

2 2.3 Venue is proper pursuant to RCW 4.12.010 and .025.

3 **III. FACTS**

4 3.1 Hold provides information security and threat intelligence services to large
5 institutional clients.

6 3.2 In early 2014, Hold, through confidential business practices and its own work
7 product, obtained access to over 360 million stolen account credentials on the Dark Web.
8 These account credentials consisted of compromised emails and passwords.

9 3.3 In early 2014, Microsoft, through its employee Simon Pope (“Pope”), contacted
10 Hold to obtain services related to recovering stolen account credentials on the Dark Web.

11 3.4 Microsoft requested services from Hold to access stolen account credentials for
12 Microsoft then-existing domains and for the protection of Microsoft customers in order to
13 prevent harm to Microsoft customers.

14 3.5 On February 26, 2014, Microsoft and Hold entered into a Non-Disclosure
15 Agreement (the “NDA”) in furtherance of Microsoft’s requests stated above.

16 3.6 Contemporaneously with the execution of the NDA, Pope transmitted an email
17 to Mr. Holden summarizing Microsoft’s promises, representations and intentions in connection
18 with the parties’ relationship and Microsoft’s treatment of the recovered stolen account
19 credentials Hold agreed to access and provide (the “Pope Email”).

20 3.7 In the Pope Email, Microsoft represents to Hold that it will “limit use of the
21 data to activities that are designed to prevent or mitigate harm to our customers.” Microsoft
22 further represents that “the data will not be used for any other purpose.” Finally, Microsoft
23 represents: “Microsoft will ensure that after the data has been used to mitigate any harm to its
24 customers, we will securely destroy all copies of the data.”

25 3.8 From February 2014 to February 2015, Hold provided Microsoft access to the
26 stolen account credentials under the NDA.

COMPLAINT - 2

SCHWABE, WILLIAMSON & WYATT, P.C.
Attorneys at Law
1420 5th Avenue, Suite 3400
Seattle, WA 98101-4010
Telephone: 206-622-1711

1 3.9 On February 6, 2015, Microsoft and Hold executed a Master Supplier Services
2 Agreement (the “2015 MSSA”), which incorporates various Statements of Work.

3 3.10 On the same day, Microsoft and Hold executed a Statement of Work (the “2015
4 SOW”) stating: “Microsoft has asked [Hold] to deliver compromised “Account Credential
5 Data” that have been recovered by [Hold] from sites on the Internet in order to reveal and
6 protect against threats to services, brands, and domains owned by Microsoft.”

7 3.11 Under these agreements between Hold and Microsoft, Hold used its products
8 and services to access and recover stolen Microsoft account credentials. The purpose of the
9 parties’ agreements, and specifically Hold’s services, was for Microsoft to match the received
10 stolen credentials with their own customers’ account credentials (in connection with agreed-
11 upon domains) in order to alert these customers of the compromised information.

12 3.12 As set out from the beginning by Pope – and as understood by Hold – any stolen
13 credentials that did not match a Microsoft account were not to be used by Microsoft and were
14 to be destroyed by Microsoft.

15 3.13 Unmatched stolen credentials are credentials that do not relate to any Microsoft
16 customers and do not belong to Microsoft. This was a critical aspect of the parties’
17 understandings and agreement. Neither Microsoft nor Hold contemplated or communicated a
18 use for the stolen account credentials outside of only protecting Microsoft’s then-existing
19 customers.

20 3.14 Microsoft’s use of stolen account credentials that do not relate to Microsoft’s
21 then-existing customers, specifically those not utilizing domains identified in the Statements
22 of Work (e.g. hotmail, live, outlook, etc.), is a violation of the parties’ agreements and of
23 Microsoft’s promises and representations.

24 3.15 Hold and Microsoft continued their respective performance pursuant to the
25 2015 MSSA and 2014 NDA, without amendment to these agreements, through and until at
26 least 2020.

COMPLAINT - 3

SCHWABE, WILLIAMSON & WYATT, P.C.
Attorneys at Law
1420 5th Avenue, Suite 3400
Seattle, WA 98101-4010
Telephone: 206-622-1711

1 3.16 Beginning in or about 2018, and without Hold’s prior knowledge, Microsoft
2 has employed an updated version of its Active Directory Federation Service (AD FS) enabling
3 federated identity and access management. Microsoft improperly and without authorization
4 utilized stolen account credentials accessed through Hold in creating this service.

5 3.17 Further, Microsoft acquired LinkedIn, which had 200 million additional users.
6 Microsoft at some point in or about 2018 improperly and without authorization, utilized stolen
7 account credentials accessed through Hold in its administration of LinkedIn.

8 3.18 Microsoft during this period also acquired Github, which had 50 million
9 additional users. Microsoft improperly and without authorization utilized stolen account
10 credentials accessed through Hold in its administration of Github.

11 3.19 Hold was not aware of Microsoft’s improper use of the stolen account
12 credentials in the AD FS, LinkedIn, and Github transactions, and, upon information and belief,
13 believes there may have been additional misuse of the data outside of those delineated above.

14 3.20 In June of 2020, Microsoft and Hold renewed its relationship and executed an
15 additional Master Supplier Services Agreement (the “2020 MSSA”).

16 3.21 On July 1, 2020, Microsoft and Hold executed a Statement of Work in
17 furtherance of the 2020 MSSA (the “2020 SOW”).

18 3.22 In July of 2020, Microsoft representatives contacted Hold with the hopes of
19 purchasing historical stolen account credentials as well as on-going access services. As the
20 data is, by its own nature, stolen, Hold was ethically and legally unable to *sell* the data itself
21 despite Microsoft’s requests. There had been prior discussions about Microsoft licensing
22 Hold’s service. However, Microsoft unilaterally cut off those negotiations and instead chose
23 to commandeer the historical data.

24 3.23 Hold then learned that Microsoft was allowing third parties to use the
25 commandeered data, and Hold’s access services, through Microsoft’s web browser Edge.

26 3.24 In Fall of 2020, Microsoft (and the U.S. Department of Defense) attempted to

1 disrupt or destroy a cyber-security threat known as TrickBot. Microsoft declared a premature
2 victory over the entities that created TrickBot in October 2020.

3 3.25 Mr. Holden, a respected figure in the cyber security world, commented to an
4 industry publication that while Microsoft's activities had achieved a level of success, the threat
5 of TrickBot was not yet a "decisive victory." As Mr. Holden predicted, the TrickBot network
6 attacked and overwhelmed U.S. Hospitals in late October 2020.

7 3.26 Microsoft seemingly took issue with Mr. Holden's public comments and
8 decided to retaliate against Hold. Microsoft employee, Richard Bosovich, on behalf of
9 Microsoft, directed Microsoft employees to cease work with Hold. This resulted in a
10 significant loss of business for Hold.

11 3.27 Further, Kevin Beaumont, Microsoft's Senior Threat Intelligence Analyst, on
12 behalf of Microsoft, tweeted false information about Hold, which resulted in Hold losing a key
13 member of its board of advisors – Brian Krebs. This resulted in additional loss of business for
14 Hold.

15 3.28 Sometime in approximately 2019/2020, unbeknownst to Plaintiff at the time,
16 Microsoft began and continued to wrongfully retain stolen account credentials in contravention
17 of the parties' agreement.

18 3.29 In early 2021, Hold discovered that Microsoft was using accessed stolen
19 account credentials outside of the scope allowed by the 2014 NDA, the 2015 MSSA, the 2015
20 SOW, the 2020 MSSA, and the 2020 SOW.

21 3.30 In early 2021, Alex Holden, the owner of Hold, contacted Microsoft regarding
22 Microsoft's out-of-scope use of the accessed stolen account credentials.

23 3.31 Microsoft refused to adhere to the agreed scope of use. Microsoft continued to
24 utilize the accessed stolen account credentials, both matched and unmatched, for its own
25 purposes.
26

1 **IV. FIRST CLAIM FOR RELIEF: Breach of the 2015 MSSA**

2 4.1 Hold incorporates all prior Paragraphs of this Complaint as if fully set forth
3 herein.

4 4.2 Microsoft and Hold entered into a written contract known as the 2015 MSSA.
5 The 2015 MSSA was renewed in 2020.

6 4.3 Pursuant to the terms of the contract, and the parties' mutually expressed
7 intentions in entering into the contract, Microsoft was to utilize the accessed stolen credentials
8 strictly for the purposes of protecting customers of Microsoft domains owned at that time.

9 4.4 Pursuant to the terms of the contract, and the parties' mutually expressed
10 intentions in entering into the contract, Microsoft would destroy any accessed stolen
11 credentials that did not match to the personal information of customers of Microsoft domains
12 owned at that time.

13 4.5 Hold and Microsoft mutually assented to the terms of the 2015 MSSA.

14 4.6 Microsoft breached the 2015 MSSA by improperly retaining customer
15 credentials accessed by Hold that did not match to the personal information of customer of
16 Microsoft domains owned at that time.

17 4.7 Microsoft breached the 2015 MSSA by utilizing the accessed stolen credentials
18 for purposes outside of the accepted scope.

19 4.8 Hold has been damaged and is entitled to monetary damages in an amount to
20 be determined at trial.

21 **V. SECOND CLAIM FOR RELIEF: Breach of the NDA**

22 5.1 Hold incorporates all prior Paragraphs of this Complaint as if fully set forth
23 herein.

24 5.2 Microsoft and Hold entered into a written contract known as the 2014 NDA.

25 5.3 The 2014 NDA is ongoing, and neither party has terminated the contract.

26 5.4 Pursuant to the terms of the contract, Microsoft agreed to not utilize, transmit,

1 or otherwise communicate information about the accessed stolen credentials to any third party
2 or for any other use outside of the uses contemplated by the parties in the 2014 NDA.

3 5.5 Hold and Microsoft mutually assented to the terms of the 2014 NDA.

4 5.6 Microsoft breached the 2014 NDA by, among other things, utilizing the
5 accessed stolen account credentials to serve Edge users, new customers from the acquisitions
6 of LinkedIn and Github, and through the creation of AD FS.

7 5.7 Hold has been damaged as a result of Microsoft's breach and is entitled to
8 monetary damages in an amount to be determined at trial.

9 **VI. THIRD CLAIM FOR RELIEF: Unjust Enrichment**

10 6.1 Hold incorporates all prior Paragraphs of this Complaint as if fully set forth
11 herein.

12 6.2 Hold conferred a benefit on Microsoft by, among other things, providing
13 Microsoft access to stolen account credentials relating to non-Microsoft domains.

14 6.3 Microsoft was able to filter the non-Microsoft domain credentials from the
15 Microsoft domain credentials.

16 6.4 Microsoft promised to destroy the non-Microsoft domain credentials.

17 6.5 Microsoft elected to not destroy the non-Microsoft domain credentials.

18 6.6 Microsoft has knowledge of the benefit received.

19 6.7 As Hold provided access to the non-Microsoft domain credentials with the
20 expectation and agreement that the credentials would be destroyed, and Microsoft wrongfully
21 retained the credentials, Microsoft is retaining the benefit under circumstances that make it
22 inequitable for them to retain them.

23 6.8 Microsoft has been unjustly enriched and Hold is entitled to damages arising
24 out of that unjust enrichment.

25 **VII. FOURTH CLAIM FOR RELIEF: Promissory Estoppel**

26 7.1 Hold incorporates all prior Paragraphs of this Complaint as if fully set forth

1 herein.

2 7.2 Microsoft promised Hold that it would destroy non-Microsoft domain
3 credentials.

4 7.3 Microsoft could reasonably have expected to cause Hold to rely on this
5 representation.

6 7.4 Hold did in fact rely on this representation.

7 7.5 Hold's reliance on this representation was reasonable.

8 7.6 As a result of that justifiable reliance, Hold has suffered damages.

9 7.7 Hold is entitled to damages in an amount to be determined at trial.

10 **VIII. FIFTH CLAIM FOR RELIEF: Tortious Interference with a Business**
11 **Expectancy**

12 8.1 Hold incorporates all prior Paragraphs of this Complaint as if fully set forth
13 herein.

14 8.2 Hold reasonably had business expectancies, and expected future opportunities
15 and profits, arising from Brian Krebs' involvement with Hold.

16 8.3 Microsoft through its agent tortiously and intentionally interfered with these
17 expectations by retaliating against Hold for Mr. Holden's factual statements regarding
18 TrickBot.

19 8.4 Microsoft tortiously and intentionally interfered with these expectations when
20 its agent and representative (Kevin Beaumont) tweeted false information in retaliation for Mr.
21 Holden's factual statements regarding TrickBot.

22 8.4 Mr. Beaumont's tweet caused Mr. Krebs to resign from Hold, leading to lost
23 revenue and profits to Hold.

24 8.5 As a result of Microsoft's tortious and intentional interference, Hold has
25 suffered damages in the form of lost revenues and profits.

26 8.6 Hold is entitled to damages in an amount to be determined at trial.

1 **IX. REQUEST FOR RELIEF**

2 WHEREFORE, Plaintiff Hold Security requests the following:

- 3 1. Judgment against Defendant in an amount to be proven at trial;
- 4 2. Pre-Judgment interest to the fullest extent allowed by law;
- 5 3. Post-Judgment interest from the date of entry of judgment until the judgment is
- 6 paid in full at the highest rate of interest allowed by law;
- 7 4. For Plaintiff's reasonable attorney fees and costs incurred in this action to the
- 8 fullest extent allowed by law; and
- 9 5. For any other relief this Court deems just and equitable.
- 10

11 Dated this 15th day of May, 2023.

12

13 SCHWABE, WILLIAMSON & WYATT, P.C.

14

15 By: s/ David R. Ebel

16 David R. Ebel, WSBA #28853

17 Email: debel@schwabe.com

18 By: s/ Davis Leigh

19 Davis Leigh, WSBA #58825

20 Email: dbleigh@schwabe.com

21 1420 5th Avenue, Suite 3400

22 Seattle, WA 98101-4010

23 Telephone: 206-622-1711

24 Facsimile: 206-292-0460

25 *Attorneys for Plaintiff*

26