Ex Baltimore Ravens Coach Indicted For Shocking And Widespread Digital Stalking Scheme

Matthew Weiss, a former Baltimore Raven and Michigan Wolverine coach is facing federal charges for an elaborate cyberstalking operation that spanned nearly eight years, targeting thousands of female college athletes across the country.

The 24-count indictment, filed March 20 in federal court, reveals a disturbing pattern of how he accessed thousands of athletes accounts through access to sensitive systems and them hacked into their email accounts to steal private intimate photos and videos.

Between 2015 and January 2023, Weiss allegedly hacked into the social media, email, and cloud storage accounts of more than 3,300 people. His primary targets were female college athletes, whom he researched based on their school affiliation, athletic history, and physical characteristics.

He also stolen PII and Medical data of more than 150,000 athletes. This included information from student athletic databases

Sophisticated Hacking Techniques

Weiss employed multiple methods to gain unauthorized access to victims' accounts. He first breached the security of athletic databases maintained by Keffer Development Services, a third-party vendor serving over 100 colleges and universities.

"Weiss obtained access to these databases through compromising the passwords of accounts with elevated levels of access, such as the accounts of trainers and athletic directors," the indictment states. This initial breach gave him personal information and medical data for more than 150,000 athletes.

The hacker then downloaded athletes' passwords that were stored in the system. Though these passwords were encrypted, Weiss allegedly cracked the encryption using research he conducted online.

Methodical Research of Victims

Weiss conducted extensive research on his targets to obtain personal details useful for password guessing. He gathered information such as mothers' maiden names, pets' names, places of birth, and nicknames.

Using this combined intelligence from athletic databases and internet research, he successfully accessed the social media, email, and cloud storage accounts of more than 2,000 targeted athletes. His method involved either guessing or resetting their passwords based on personal information he had gathered.

The indictment details how Weiss created detailed notes on his victims. He kept records commenting on their bodies and sexual preferences after viewing their private photos and videos.

University Systems Compromised

The University of Michigan was among the educational institutions targeted by Weiss. In December 2022, he allegedly reset passwords for more than 40 email accounts belonging to University of Michigan alumni.

"After resetting the passwords of more than 40 email accounts of University of Michigan alumni, Weiss accessed more than 25 of these accounts," the court document states. This access allowed him to search for private photographs and videos not meant for public sharing.

Weiss also targeted Westmont College, compromising the accounts of at least five students or former students. His unauthorized access spanned multiple technology providers and university systems across the country.

Read Whole Indictment On Following Pages

15

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

Case: 2:25-cr-20165
Assigned To : Edmunds, Nancy G.
Referral Judge: Patti, Anthony P.
Assign. Date : 3/20/2025
Description: INDI USA V. WEISS (NA)

United States of America,

Plaintiff,

v.

Matthew Weiss,

Defendant.

_____/

Violations:
18 U.S.C. § 1030(a)(2)(c)
18 U.S.C. § 1030(c)(2)(B)(ii)
18 U.S.C. § 1028A(a)(1)

INDICTMENT

THE GRAND JURY CHARGES:

THE DEFENDANT'S SCHEME

1. Between approximately 2015 and January 2023, Matthew Weiss gained access—without and in excess of authorization—to the social media, email, and/or cloud storage accounts of more than 3,300 people.

2. Weiss primarily targeted female college athletes. He researched and targeted these women based on their school affiliation, athletic history, and physical characteristics. His goal was to obtain private photographs and videos never intended to be shared beyond intimate partners.

3. Through this scheme, unknown to account holders, Weiss downloaded personal, intimate digital photographs and videos.

4. Weiss researched the targeted athletes on the internet. Months—and in some cases years—after he gained access to certain accounts, he returned to those accounts searching for additional photos and videos.

5. Weiss kept notes on individuals whose photographs and videos that he viewed, including notes commenting on their bodies and their sexual preferences.

THE DEFENDANT'S ACCESS TO ACCOUNTS BY WAY OF ATHLETE DATABASES

6. Weiss obtained access—without and in excess of authorization—to student athlete databases of more than 100 colleges and universities across the country that were maintained by Keffer Development Services, a third-party vendor. Weiss obtained access to these databases through compromising the passwords of accounts with elevated levels of access, such as the accounts of trainers and athletic directors.

7. After gaining access to these databases, Weiss downloaded the personally identifiable information (PII) and medical data of more than 150,000 athletes.

8. Weiss also downloaded passwords that athletes used to access Keffer Development Services' system to view and update the athletes' data. The athletes' passwords that Weiss downloaded were encrypted. Weiss cracked the encryption protecting the passwords, assisted by research that he did on the internet.

9. Through open-source research—and through information that appeared to be leaked from data breaches—Weiss conducted additional research on targeted

athletes to obtain personal information such as their mothers' maiden names, pets, places of birth, and nicknames.

10. Using the combined information that he obtained from the student athlete databases and his internet research, Weiss was able to obtain access to the social media, email, and/or cloud storage accounts of more than 2,000 targeted athletes by guessing or resetting their passwords.

11. Once he obtained access to the accounts of targeted athletes, Weiss searched for and downloaded personal, intimate photographs and videos that were not publicly shared.

THE DEFENDANT'S ACCESS BY WAY OF COMPROMISING STUDENT/ALUMNI ACCOUNTS

12. Weiss also obtained access—without and in excess of authorization—to the social media, email, and/or cloud storage accounts of more than 1,300 additional students and/or alumni from universities and colleges from around the country.

13. Once Weiss gained access to these accounts, he would search for and download personal, intimate photographs and videos.

14. In at least several instances, Weiss exploited vulnerabilities in universities' account authentication processes to gain access to the accounts of students or alumni. Weiss leveraged his access to these accounts to gain access to other social media, email, and/or cloud storage accounts.

COUNTS ONE THROUGH TEN

Unauthorized Access
18 U.S.C. § 1030(a)(2)(c) and (c)(2)(B)(ii)

15. Paragraphs 1 through 14 are incorporated by reference.

16. From in and around 2015, to in and around January 2023, in the Eastern District of Michigan and elsewhere, Matthew Weiss intentionally accessed—without and in excess of authorization—protected computers (as that term is defined in Title 18, United States Code, Section 1030(e)(2)), including servers from identified and unidentified social media, email, and/or cloud storage providers. Weiss thereby obtained digital photographs, videos, and other private information belonging to more than 3,300 individuals in furtherance of tortious acts, including violations of the Michigan and Maryland state torts of Invasion of Privacy.

17. The chart below sets forth individualized facts of Counts 1 through 10.

Count	Date (in and around)	Targeted Individual	Targeted Server
1	May 2021 to January 2023	Jane Doe #1	Unknown Technology Provider
2	July 2021 to January 2023	Jane Doe #2	Technology Provider #1
3	October 2022	Jane Doe #3	Technology Provider #2
4	December 2022	Jane Doe #4	University of Michigan
5	December 2022	Jane Doe #5	Technology Provider #3
6	July 2022 to January 2023	Jane Doe #6	Unknown Technology Provider
7	October 2022	Jane Doe #7	Technology Provider #1
8	September 2021	Jane Doe #8	Technology Provider #1
9	August 2021 to January 2023	Jane Doe #9	Technology Provider #1
10	November 2022	Jane Doe #10	Technology Provider #1

All in violation of 18 United States Code, Sections 1030(a)(2)(c) and 1030(c)(2)(B)(ii).

COUNTS ELEVEN THROUGH TWENTY

Aggravated Identity Theft
18 U.S.C. § 1028A(a)(1)

18. Paragraphs 1 through 17 are hereby incorporated by reference.

19. From in and around May 2021, to in and around January 2023, in the Eastern District of Michigan and elsewhere, Matthew Weiss, during and in relation to felony violations of Title 18, United States Code, Sections 1030(a)(2)(c) and 1030(c)(2)(B)(ii), did knowingly transfer, possess and use, without lawful authority, the means of identification of the other persons identified in the chart below, that may be used—alone and in conjunction with other information—to identify the other persons identified below, each such means of identification representing a separate count herein.

20. The chart below sets out individualized facts of Counts 11 through 20.

Count	Date (in and around)	Targeted Individual	Means of Identification
11	May 2021	Jane Doe #1	Login identifier for Unknown Technology Provider
12	July 2021 to January 2023	Jane Doe #2	Login identifier for Technology Provider #1
13	October 2022	Jane Doe #3	Login identifier for Technology Provider #2
14	December 2022	Jane Doe #4	University unique identifier
15	December 2022	Jane Doe #5	Login identifier for Technology Provider #3
16	July 2022 to January 2023	Jane Doe #6	Login identifier for Unknown Technology Provider
17	October 2022	Jane Doe #7	Login identifier for Technology Provider #1
18	September 2021	Jane Doe #8	Login identifier for Technology Provider #1
19	August 2021 to January 2023	Jane Doe #9	Login identifier for Technology Provider #1
20	November 2022	Jane Doe #10	Login identifier for Technology Provider #1

All in violation of 18 United States Code, Section 1028A(a)(1).

COUNT TWENTY-ONE

Unauthorized Access
18 U.S.C. § 1030(a)(2)(c) and (c)(2)(B)(ii)

21. Paragraphs 1 through 14 are hereby incorporated by reference.

22. From in and around January 2020, to in and around October of 2021, in the Eastern District of Michigan and elsewhere, Matthew Weiss intentionally accessed —without and in excess of authorization—protected computers (as that term is defined in Title 18, United States Code, Section 1030(e)(2)), that is, virtual server space rented by the company Keffer Development Services. After compromising the passwords of approximately 150 accounts and gaining access to these same accounts, Weiss downloaded personally identifiable information (PII) and medical data of more than 150,000 athletes in furtherance of tortious acts, including violations of the Maryland, Michigan, and Pennsylvania state torts of Invasion of Privacy. The offense was committed in furtherance of additional violations of 18 U.S.C. §§ 1030(a)(2)(c) to wit, Matthew Weiss intended to and did obtain information that furthered his ability to reset the passwords for and access—without and in excess of authorization— social media, email, and/or cloud storage accounts of individuals whose information he obtained from Keffer's systems.

All in violation of 18 United States Code, Sections 1030(a)(2)(c) and 1030(c)(2)(B)(ii).

COUNT TWENTY-TWO

Unauthorized Access
18 U.S.C. § 1030(a)(2)(c) and (c)(2)(B)(ii)

23. Paragraphs 1 through 14 are hereby incorporated by reference.

24. From in and around October 2022, to in and around January 2023, in the Eastern District of Michigan and elsewhere, Matthew Weiss intentionally accessed—without and in excess of authorization—protected computers (as that term is defined in Title 18, United States Code, Section 1030(e)(2)), that is, servers operated by Technology Provider #1, and obtained digital photographs, videos, and other private information of the provider's customers. Weiss accessed the accounts belonging to more than forty of the provider's customers in furtherance of tortious acts, including violations of the Michigan state tort of Invasion of Privacy.

All in violation of 18 United States Code, Sections 1030(a)(2)(c) and 1030(c)(2)(B)(ii).

COUNT TWENTY-THREE

Unauthorized Access
18 U.S.C. § 1030(a)(2)(c) and (c)(2)(B)(ii)

25. Paragraphs 1 through 14 are hereby incorporated by reference.

26. From in and around December 21, 2022, to in and around December 23, 2022, in the Eastern District of Michigan and elsewhere, Matthew Weiss intentionally accessed—without and in excess of authorization—protected computers (as that term is defined in Title 18, United States Code, Section 1030(e)(2)), that is, servers of the University of Michigan and its email provider. After resetting the passwords of more than 40 email accounts of University of Michigan alumni, Weiss accessed more than 25 of these accounts in furtherance of tortious acts, including violations of the Michigan state tort of Invasion of Privacy. The offense committed in furtherance of additional violations of 18 U.S.C. §§ 1030(a)(2)(c), to wit, Matthew Weiss intended to and did obtain information that furthered his ability to access—without and in excess of authorization—one or more social media, email, and/or cloud storage accounts of one or more University of Michigan alumni.

All in violation of 18 United States Code, Sections 1030(a)(2)(c) and 1030(c)(2)(B)(ii).

COUNT TWENTY-FOUR

Unauthorized Access
18 U.S.C. § 1030(a)(2)(c) and (c)(2)(B)(ii)

27. Paragraphs 1 through 14 are hereby incorporated by reference.

28. From in and around October 2022, to in and around January 2023, in the Eastern District of Michigan and elsewhere, Matthew Weiss intentionally accessed—without and in excess of authorization—protected computers (as that term is defined in Title 18, United States Code, Section 1030(e)(2)), that is, servers of Westmont College and its email provider. Weiss accessed the accounts of more than five Westmont students or former students in furtherance of tortious acts, including violations of the California and Michigan state torts of Invasion of Privacy. The offense was committed in furtherance of additional violations of 18 U.S.C. §§ 1030(a)(2)(c) and (a)(5)(A), to wit, Matthew Weiss intended to and did obtain information that furthered his ability to access—without and in excess of authorization— one or more social media, email, and/or cloud storage accounts of one or more Westmont College students or former students.

All in violation of 18 United States Code, Sections 1030(a)(2)(c) and 1030(c)(2)(B)(ii).

FORFEITURE ALLEGATIONS

Criminal Forfeiture
18 U.S.C. § 982(a)(2)(B) and 1030(i)

29. The allegations contained in Counts One through Twenty-Four of this Indictment are incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i).

30. Upon conviction of one or more of the unauthorized access offenses in violation of Title 18, United States Code, Section 1030(a)(2)(c) and (c)(2)(B)(ii), set forth in this Indictment, defendant Matthew Weiss shall forfeit to the United States of America:

a. pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of such offense; and

b. pursuant to Title 18, United States Code, Section 1030(i), any personal property that was used or intended to be used to commit or to facilitate the commission of such offense.

The property to be forfeited includes, but is not limited to, all electronic devices and online accounts used or intended to be used to facilitate unauthorized access to accounts belonging to other individuals.

31. If any of the property described above, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b) and 1030(i).

All pursuant to Title 18, United States Code, Sections 982(a)(2)(B), 982(b), 1030(i), and Title 21, United States Code, Section 853.

THIS IS A TRUE BILL

s/Grand Jury Foreperson
GRAND JURY FOREPERSON

JULIE A. BECK
Acting United States Attorney

s/ Mark Chasteen
MARK CHASTEEN
Chief, White Collar Crime Unit
Assistant United States Attorney

s/ Timothy J. Wyse
TIMOTHY J. WYSE
Assistant United States Attorney

Dated: March 20, 2025