

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA,

Plaintiff,

vs.

KEVIN CAVE,

Defendant.

8:12CR417

FINDINGS AND
RECOMMENDATIONS

This matter is before the court on the Motion to Dismiss ([Filing No. 22](#)) filed by defendant Kevin Cave (Cave). Cave is charged in the Superseding Indictment ([Filing No. 9](#)) with intentionally exceeding authorized access to a protected computer for private financial gain in violation of [18 U.S.C. §1030\(a\)\(2\)\(C\)](#) and [\(c\)\(2\)\(B\)\(i\)](#). Cave moves to dismiss the Superseding Indictment ([Filing No. 9](#)) because the Superseding Indictment fails to state an offense. Cave asserts the Superseding Indictment only alleges a misappropriation of information which is not a criminal act under the Computer Fraud and Abuse Act (CFAA). Cave submitted a brief ([Filing No. 23](#)) in support of his motion. The government submitted a brief ([Filing No. 25](#)) in response to the motion.

The court held a hearing on May 7, 2013. Cave was present with his counsel, Emil M. Fabian. Assistant United States Attorney Jan W. Sharp represented the United States. The parties did not present any evidence. A transcript (TR.) of the hearing was prepared and filed on May 13, 2013 ([Filing No. 29](#)), upon which the motion was deemed submitted.

FINDINGS OF FACT

According to the Superseding Indictment, Cave was an officer with the Omaha Police Department (OPD) from September 23, 2002, until September 7, 2012. **See** [Filing No. 9](#) - Superseding Indictment ¶ 9. While working for OPD, Cave underwent training on the use of the Nebraska Criminal Justice Information System database (NCJIS). *Id.* NCJIS allows approved agencies to link to databases that provide information including criminal history information, driver's license information, employment information, information from penal institutions, and probation and parole

information. *Id.* ¶ 2. Before accessing NCJIS, approved agencies must sign a memorandum of understanding (MOU) acknowledging the confidentiality of the information found on NCJIS. See [Filing No. 9](#) - Superseding Indictment ¶ 5. Approved agencies then train users within the agency on these regulations. *Id.* Information found within NCJIS is for use by law enforcement personnel within their official capacity only and is not to be made public. *Id.* ¶ 7.

OPD is an agency authorized to use NCJIS. *Id.* ¶ 8. Cave completed training and was authorized to use NCJIS on January 24, 2008, and remained authorized until September 7, 2012. *Id.* ¶ 9. The government alleges that beginning on March 2, 2010, until August 21, 2012, Cave conducted unauthorized NCJIS database searches in an effort to locate certain individuals and disseminated the information to car dealerships attempting to repossess vehicles. *Id.* ¶ 10. The government alleges the car dealerships paid Cave up to \$200.00 for each lead and that he received a total of about \$16,050.00. *Id.* ¶ 11. The government alleges Cave violated [18 U.S.C. §1030\(a\)\(2\)\(C\)](#) and [\(c\)\(2\)\(B\)\(i\)](#) by exceeding his authorized access to NCJIS and obtaining information that he then made public for personal financial gain. *Id.* ¶ 12.

ANALYSIS

Cave asserts that the Superseding Indictment should be dismissed because it “fails to state an offense for the reason the government has pled facts tending to show that the defendant misappropriated information, not that he was without authorization or exceeded his authorization in accessing such information.” See [Filing No. 22](#) - Motion. Cave contends that he did not “exceed authorized access” within the plain meaning of the phrase under the CFAA. *Id.* Cave also contends that legislative history leans towards a narrow interpretation of the phrase “exceeds authorized access” which would exclude the misuse of information from the scope of the CFAA. *Id.*

A. Legislative History

Cave contends that looking into legislative history behind the CFAA would support taking a more narrow interpretation of the phrase “exceeds authorized access”. See [Filing No. 23](#) - Brief p. 6. Cave alleges that the original purpose of the statute was

“intended to prohibit electronic trespassing, not the subsequent use or misuse of information.” *Id.* (citing *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 966 (D. Ariz. 2008)). Cave contends that had Congress wanted to make misuse of information a criminal act under the CFAA it would have done so. **See** [Filing No. 23](#) - Brief p. 6.

In 1986 the Senate changed the wording of the CFAA. In Senate Report No. 99-432, the Senate explained, “Section 2(c) substitutes the phrase ‘exceeds authorized access’ for the more cumbersome phrase in present 18 U.S.C. § 1030(a)(1) and (a)(2), ‘or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend’. The Committee intends this change to simplify the language[.]” S. Rep. No. 99-432, at *9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2486. Cave contends that through this change the Senate meant to eliminate coverage of the phrase, “or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend.” **See** [Filing No. 23](#) - Brief p. 6. Cave asserts that because the coverage of this phrase is eliminated, if Congress had intended this area to be covered Congress would have included coverage under the statute. *Id.*

Cave also relies upon a separate writing by Senators Mathias and Leahy (the Senators) in which the Senators said, “This removes from the sweep of the statute one of the murkier grounds of liability, under which a Federal employee’s access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization.” S. Rep. No. 99-432, at *21.

In the 1986 Senate report, the Senators stated that the reasoning behind changing the language was only “to simplify the language” and not to change the scope of the coverage as alleged by the defendant. The separate writing by the Senators were written about 18 U.S.C. § 1030(a)(3), which had also been amended that day. When amending § 1030(a)(3) the Senate changed the mens rea requirement from knowingly use to intentionally use. **See** S. Rep. No. 99-432, at *21. Cave takes this to enforce his position that the Senate meant to remove the phrase completely from the scope of coverage of the statute. **See** [Filing No. 23](#) - Brief p. 6. The Senators wrote

about the murky area in which those who did not intend to access the information could be charged under § 1030(a)(3).

Cave is not being charged under § 1030(a)(3), instead he is being charged under 18 U.S.C. § 1030(a)(2)(C), therefore the writing of the Senators does not have any application to his case. Also, because the intent of the legislature as to 18 U.S.C. § 1030(a)(2) was only to simplify the language, the scope of coverage was not changed, therefore using access for purposes to which authorization does not extend remains within the scope of the CFAA.

B. Meaning of “Exceeds Authorized Access”

Title 18 of the U.S.C. § 1030 provides, “Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains . . . information from any protected computer . . . shall be guilty of a felony.” The phrase “exceeds authorized access” as defined in the statute means, “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.” [18 U.S.C. § 1030\(a\)\(2\)\(C\)](#). “A person is ‘without authorization’ when an individual either (1) has never been granted access to the computer yet obtains access to the computer without the access-grantor’s permission, or (2) has been granted access as the access-grantor’s agent but loses authorization to access the computer when the agent breaches his duty of loyalty.” *NCMIC Fin. Corp. v. Artino*, 638 F. Supp. 2d 1042, 1057 (S.D. Iowa 2009). “Both inquiries focus on a person’s intent at the time of accessing the computer, not on a person’s subsequent misappropriation of the information or thing of value obtained from the employer’s computer.” *Id.* at 1059.

Cave contends that since he at no time altered any information on the database or at no time did he lack the authorization to obtain information from NCJIS, he did not “exceed authorized access” according to the statute. See [Filing No. 23](#) - Brief p. 2. Additionally, Cave asserts he was granted full access to the information on the database, thus he did not exceed his authorized use. See [Filing No. 29](#) - TR. p. 3, 9-14.

The government contends that Cave did not have authorization to access the information to begin with because the search was done for an improper purpose. *Id.* at

6, 7-8. The government does not allege that Cave conducted a proper search and then misused the information; instead the government alleges that the search was improper from the start. **See** [Filing No. 25](#) - Response p. 5. The government contends that Cave's searches were not connected to any legitimate law enforcement activity, and therefore were not authorized. *Id.* at 15.

When OPD obtained access to NCJIS, OPD signed a MOU. The MOU specifically stated use of NCJIS is "for the purpose of improving public safety and improving the ability of criminal justice agencies in the performance of their official duties." **See** [Filing No. 25](#) - Response p. 2. After OPD signed the MOU and obtained access to NCJIS, OPD trained their officers on the rules and regulations prescribed in the MOU, specifically addressing regulations pertaining to access and disclosure and the confidential nature of the information found on NCJIS **See** [Filing No. 9](#) - Superseding Indictment ¶¶ 5, 8. Cave allegedly accessed confidential information available through NCJIS and provided such information to car dealerships attempting to repossess vehicles. *Id.* ¶ 10. In return, Cave allegedly received money. *Id.* ¶ 11. OPD granted Cave access to NCJIS for the limited purposes set forth in the MOU, specifically, for the purpose of "improving the ability of criminal justice agencies in the performance of their official duties." Cave's actions, if proven, fit within the definition of "exceeds authorized access" because accessing confidential information for personal financial gain is not within the aforementioned purpose.

C. Failure to State an Offense

Cave argues that the Superseding Indictment fails to set forth sufficient facts and allegations as to the violation of the CFAA, and that the Indictment fails to state a plain, concise, and definite written statement of essential facts constituting an offense pursuant to Fed.R.Crim.P. 12(b)(3)(B). **See** [Filing No. 22](#) - Motion. Cave alleges "the Superseding Indictment failed to state an offense for the reason that the government has pled facts tending to show that the Defendant misappropriated information, not that he was without authorization or exceeded his authorization in accessing such information." *Id.*

“An indictment is sufficient if it contains all of the essential elements of the offense charged, fairly informs the defendant of the charges against which he must defend, and alleges sufficient information to allow a defendant to plead a conviction or acquittal as a bar to a subsequent prosecution.” *United States v. Sohn*, 567 F.3d 392, 394 (8th Cir. 2009). “[A]n indictment is normally sufficient if its language tracks the statutory language.” *United States v. Hayes*, 574 F.3d 460, 472 (8th Cir. 2009). In this case, the Superseding Indictment satisfies the elements of a constitutionally sufficient indictment and concisely follows the statutory language of the CFAA.

The Superseding Indictment mirrors the statutory language of the CFAA. The CFAA requires that the defendant intentionally access and obtain information, without authorization or exceeding authorization, from a protected computer and that it be done for personal financial gain. See [18 U.S.C. §1030\(a\)\(2\)\(C\)](#) and [\(c\)\(2\)\(B\)\(i\)](#). Those elements are specifically stated in the Superseding Indictment and inform Cave of the charges against him. See [Filing No. 9](#) - Superseding Indictment ¶ 12. The Superseding Indictment also includes specific elements as to Cave’s CFAA violation. *Id.* ¶¶ 9-12. According to the Superseding Indictment, the violation began on or about March 10, 2010, and continued until on or about August 21, 2012. *Id.* ¶ 10. The dates of the violation gave adequate notice of when the alleged offense occurred and enabled Cave to respond to the charges without fear of a subsequent prosecution for the same crime. The Superseding Indictment sets forth sufficient facts and allegations that if proven could constitute a violation of [18 U.S.C. §1030\(a\)\(2\)\(C\)](#) and [\(c\)\(2\)\(B\)\(i\)](#). Accordingly,

IT IS RECOMMENDED TO JUDGE JOSEPH F. BATAILLON that:

Kevin L. Cave’s Motion to Dismiss for Failure to State an Offense ([Filing No. 22](#)) be denied.

ADMONITION

Pursuant to NECrimR 59.2 any objection to this Findings and Recommendation shall be filed with the Clerk of the Court within fourteen (14) business days after being served with a copy of this Findings and Recommendation. Failure to timely object may constitute a waiver of any objection. The brief in support of any objection shall be filed

at the time of filing such objection. Failure to file a brief in support of any objection may be deemed an abandonment of the objection.

Dated this 29th day of May, 2013.

BY THE COURT:

s/ Thomas D. Thalken
United States Magistrate Judge