

433 F.3d 1057

United States Court of Appeals,
Eighth Circuit.

UNITED STATES of America, Appellee,
v.
Thomas S. MILLOT, Appellant.

Filed: Jan. 9, 2006.

Before SMITH, HEANEY, and BENTON,
Circuit Judges.

HEANEY, Circuit Judge.

On June 15, 2004, a jury found Thomas S. Millot guilty of unauthorized computer intrusion, in violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(a)(5)(A)(ii), (a)(5)(B)(i), and (c)(4)(B). The district court sentenced Millot to three months of imprisonment, three months of home detention, three years of supervised release, a \$5,000 fine, and restitution in the amount of \$20,350. Millot appeals his conviction, sentence, and restitution order, alleging several errors by the district court. We affirm.

BACKGROUND

In 2000, Millot worked as a systems analyst in the Information Access Management Group for Aventis Pharmaceuticals. The Information Access Management Group managed the day-to-day computer security duties at Aventis's Kansas City, Missouri facility. Millot was responsible for administration of the SecureID cards and accounts. A SecureID card is an active device that generates a number that, in combination with a user name and personal identification number, allows Aventis employees to remotely access the Aventis computer system in order to check email and perform other job-related functions. An employee's remote access level depends on the individual's responsibilities for the company. As a systems analyst, Millot's access level was the highest available.

Millot had the lead responsibility for disabling remote access accounts when individuals left employment and collecting and tracking returned SecureID cards. On or around August 2000, Millot reassigned the access account of former employee Gernot Fromm to one of the inventoried SecureID cards, and increased the account access level to the highest level available.

In October of 2000, Aventis Pharmaceuticals outsourced its security functions to International Business Machines (IBM). Although several members of the Information Access Group were subsequently hired by IBM, Millot was not offered a job with IBM, and left employment with Aventis in September 2000. When he left employment, he kept the SecureID card he assigned to the Fromm account. To keep the card active he periodically accessed the network. Millot used the Fromm account to access the Aventis computer network nine times between August 26 and December 16, 2000. On December 16, 2000, he used the SecureID card and the Fromm account to log onto the Aventis system and delete Jeff Jernigan's account. Jernigan was the manager of Technical Services for Aventis, and his ability to remotely access and monitor the network was essential to his job. December 16, 2000, was a Saturday, and Jernigan unsuccessfully attempted to access the Aventis system from his home. Although Geoffrey Bridges was able to rebuild Jernigan's account within a matter of hours, Jernigan continued to experience problems with his account for the following three weeks.

Bridges and Lori Meyer, former Aventis employees then working for IBM, performed the bulk of the activities in response to Millot's intrusion into the Aventis computer system. Bridges rebuilt the Jernigan account and investigated the intrusion while Meyer performed a security audit to verify that all existing access accounts belonged to current employees, and that each account's access level was appropriate. Bridges spent 31 hours restoring Jernigan's account and investigating the computer intrusion, and Meyers spent 376 hours on the audit for a total of 407 hours. IBM billed its

staff's services at fifty dollars per hour, for a total cost of \$20,350.

Investigators traced the unauthorized remote access back to Millot's personal internet access account. On March 3, 2003, Millot confessed that he had taken over the Fromm account, repeatedly contacted the Aventis computer system, and deleted the Jernigan account. The grand jury issued an indictment alleging that "it cost more than Five Thousand Dollars (\$5,000) [to at least one or more persons] to conduct a damage assessment of, verify the security of, and restore the integrity of the Aventis network computer system."

Millot admitted the underlying conduct, but challenged the government's allegation that the loss caused by his conduct amounted to the \$5,000 minimum required for a conviction under the CFAA. Following a two-day trial, the jury found the loss exceeded \$5,000 and found Millot guilty of the charged offense. His base offense level was 6, with a four-level enhancement for loss more than \$10,000 but less than \$30,000, a two-level enhancement for abuse of position of trust, and a two-level adjustment for acceptance of responsibility. Accordingly, his adjusted offense level was 10 with a criminal history category of I, resulting in a sentencing range of 6 to 12 months. On November 10, 2004, the district court sentenced Millot to a split sentence, at the bottom of the range, of three months of imprisonment, three months of home detention, and three years supervised release. The district court also ordered Millot to pay a \$5,000 fine and \$20,350 in restitution for the time spent by Bridges and Meyers. This appeal followed.

ANALYSIS

Millot alleges the government failed to prove damage of at least \$5,000 because the district court erred in finding IBM a "victim" under the CFAA. He also alleges that the district court erred in sentencing him under the pre-Booker mandatory sentencing guidelines, and that the restitution order also violated Booker.

I. Millot's Conviction Under the CFAA

To determine whether we should overturn Millot's conviction, we must determine whether the district court properly classified IBM as a potential victim under the CFAA, and if so, whether the government's evidence was sufficient for a jury to find that the loss exceeded \$5,000.

We review the district court's interpretation of a statute de novo, *see United States v. Moore*, 38 F.3d 977, 979 (8th Cir.1994), and in reviewing a jury verdict, we "view the evidence in the light most favorable to the jury's verdict, overturning it only if no reasonable jury could conclude that the government has proven all the elements beyond a reasonable doubt," *United States v. Cole*, 380 F.3d 422, 425 (8th Cir.2004).

Millot argues that any costs incurred by IBM should not have been considered in determining whether the loss amounted to the statutory minimum because the system was owned by Aventis and IBM was a "volunteer" fixing the system. This argument lacks merit. The CFAA provides for a fine and imprisonment up to five years for an individual who "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage" and that conduct causes "loss to 1 or more persons during any 1-year period ... aggregating at least \$5,000 in value." 18 U.S.C. §§ 1030(c)(4)(B), (a)(5)(A)(ii), (a)(5)(B)(i) (emphasis added). Although the damage was done to the Aventis computer system, the statute does not restrict consideration of losses to only the person who owns the computer system, and the district court properly instructed the jury to consider losses sustained by IBM in determining whether the statutory minimum was met.

Next we address the sufficiency of the evidence. Millot contends that the government's evidence was insufficient to establish that the actual loss exceeded the \$5,000 minimum, because there was no evidence that IBM specifically billed Aventis the amount alleged. The Ninth Circuit addressed a similar challenge in *United States v. Middleton*, 231 F.3d 1207,

1213-14 (9th Cir.2000). There, the defendant argued that since salaried employees fixed the damage caused by the defendant's conduct, the government could not prove that the defendant had caused damage in excess of the \$5,000 minimum. *Id.* The Ninth Circuit disagreed, stating "whether the amount of time spent by the employees and their imputed hourly rates were reasonable for the repair tasks that they performed are questions to be answered by the trier of fact." *Id.* at 1214. There, the value of the loss was calculated by multiplying the number of hours spent repairing the damage by an estimated hourly rate based on the employees' annual salary. *Id.* at 1213. The Ninth Circuit stated that "[t]here is no basis to believe that Congress intended the element of 'damage' to depend on a victim's choice whether to use hourly employees, outside contractors, or salaried employees to repair the same level of harm to a protected computer." *Id.* at 1214.

At Millot's trial, the government presented undisputed evidence regarding the hours spent by Bridges and Meyers in response to the unauthorized intrusion, and that the time spent was valued at fifty dollars per hour. IBM undoubtedly paid Meyers and Bridges for their time, and the work was done on behalf of Aventis to remedy damage to Aventis's computer system that Millot admits he caused. Millot's own expert agreed that the work done by Meyers and Bridges was a reasonable response to the discovery of a breach in the security of the computer system. Millot argues that the cost of the work performed was absorbed by IBM under its existing contract with Aventis. This argument neglects the fact that the hours spent by Bridges and Meyers addressing the issues caused by Millot's unauthorized intrusion could have been spent on other duties under the contract. *See United States v. Sablan*, 92 F.3d 865, 870 (9th Cir.1996) (holding it proper to base the estimated cost of repairs on the standard hourly rate for the employees who fixed the problem, because their time would have otherwise been devoted to assisting bank customers).

Accordingly, we find that the evidence presented was sufficient to support the conviction.

[. . .]

CONCLUSION

For the above-stated reasons we affirm the district court.