

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA

v.

FRANCIS G. JANOSKO,

Defendant

Case No. **CR 10.323. GAO**

VIOLATIONS:

**18 U.S.C. § 1030(a)(5)(A)(i), (a)(5)(B)(i),
(a)(5)(B)(v), (b) (Intentionally Damaging a
Protected Computer)**

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

18 U.S.C. § 2 (Aiding and Abetting)

INDICTMENT

The Grand Jury charges as follows:

1. During all relevant times, FRANCIS G. JANOSKO was an inmate at the Plymouth County Correctional Facility in Plymouth County, Massachusetts.
2. The prison provided JANOSKO's unit a computer so the inmates could research legal matters.
3. Since the prison was concerned with computer and prison security, it wanted the computer to give inmates access to legal research but nothing else. As configured, the computer did not give inmates access to the Internet, to other computers on the prison's networks, or even to other computer programs on the legal research computer.
4. The prison attempted to meet its security needs using several measures:
 - a. The computer located in JANOSKO's unit was a "thin client," meaning that it did not run programs or store data itself, but rather accessed programs and data over a network from a central legal research computer server located outside JANOSKO's unit.
 - b. The legal research program had been selected to avoid Internet access, because it searched only legal resources within the prison's own computer system, which it updated as needed from CD-ROMs, rather than from the Internet.
 - c. Prison personnel configured the program and network to give the inmates access to only the legal research program, and no other computer program. Even quitting the

program would not give the inmates access to a conventional Windows “desktop” with the normal Internet and other programs that Windows computers generally have. Instead, quitting the program would bring up a blue screen with only one choice, to enter the legal research program again.

d. Although the legal research computer server was connected through the prison’s network to the Internet solely so that it could obtain updates to its Windows operating system, the legal research server was configured to disallow access to the Worldwide Web, the network of websites that people outside prisons commonly access (such as websites with addresses beginning with the “www.” prefix). The legal research server was configured to not even offer inmates an Internet browser or e-mail program.

e. The legal research program existed on its own physical computer, separate from the servers that provided prison personnel e-mail and website access to the outside world.

f. Although the legal research server connected to the same physical network as the prison’s other computer servers, the prison attempted to configure the network so that inmates could not “tunnel” from the legal research server to the prison’s other computers.

g. Prison rules also prohibited inmates from possessing or using any item that was altered from its original state, from misusing any item, and from using an item for anything other than its intended use.

5. Despite these restrictions, JANOSKO figured out how to use the legal research computer in his unit for purposes other than legal research.

6. JANOSKO did so by several methods, including exploiting an idiosyncrasy in the legal research software that the prison personnel did not previously know about.

7. Between October 1, 2006 and February 7, 2007, JANOSKO used these methods to:

a. Configure the prison’s computer network to provide himself and the other inmates in his unit access to programs other than the legal research program;

b. Access, attempt to access, and provide inmates access to information and computer files from the prison's computer network and the Internet other than legal research;

c. Access, attempt to access, and provide inmates access to a report listing the names, dates of birth, Social Security numbers, home addresses and telephone numbers, and past employment history of over 1,100 current and former prison personnel;

d. Configure the prison's computer network to provide himself and other inmates access to the information listed in the prior subparagraphs;

e. Obtain the username and password to an important prison management computer program;

f. Attempt to log in to that program (fortunately without success up to the point that he was caught);

h. Attempt to send two e-mails outside the prison (neither of which contained the sensitive data identified below);

g. Download two short video files from the Internet;

i. Access, attempt to access, and provide inmates access to digital photographs of two prison personnel, two inmates, and one (publicly-available) aerial shot of the prison itself; and

j. Configure the prison's computer network to provide himself and other inmates access to the photographs listed in the prior subparagraph.

8. All these actions were unauthorized and in excess of JANOSKO's authorized access to the prison's computer network.

9. On or about February 7, 2008, JANOSKO possessed a piece of paper in his cell that bore the username and password to the prison management computer program. JANOSKO was not authorized to possess this password or to access that application.

10. Through the above actions, JANOSKO caused and attempted to cause loss to the Plymouth County Correctional Facility during a 1-year period aggregating at least \$5,000 in value.

11. The legal research server and other computers that JANOSKO accessed were used in interstate and foreign communication.

COUNT 1
Intentionally Damage to a Protected Computer
18 U.S.C. §§ 1030(a)(5)(A)(i),¹ (a)(5)(B)(i), (a)(5)(B)(v), (b) and 2

12. The Grand Jury realleges and incorporates by reference the allegations in paragraphs 1-11 of this Indictment and charges that:

From approximately October 1, 2006 through February 7, 2007, in the District of Massachusetts and elsewhere, the defendant,

FRANCIS G. JANOSKO,

knowingly caused and attempted to cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused and attempted to cause damage without authorization to a protected computer — that is, the legal research server and other servers used by the Plymouth County Correctional Facility and used in interstate and foreign communication — and caused and would have caused damage by (a) impairing the integrity and availability of the prison's information, computer programs, and computer network through configuring the prison's computer network to provide himself and the other inmates in his unit access to programs other than the legal research program; (b) configuring the prison's computer network to provide himself and other inmates access to photographs and a report listing the names, dates of birth, Social Security numbers, home addresses and telephone numbers, and past employment history of over 1,100 current and former prison personnel; and (c) attempting to log in to an important prison management computer program. This damage affected and would have affected a computer system used by and for a government entity in furtherance of the administration of justice, and, during a 1-year period, caused and attempted to cause loss to the Plymouth County Correctional Facility aggregating at least \$5,000 in value.

All in violation of Title 18, United States Code, Section 1030(a)(5)(A)(i), (a)(5)(B)(i), (a)(5)(B)(v), (b) and 2.

¹ All citations to 18 U.S.C. § 1030(a)(5) refer to the statute before it was amended by the Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110-326 § 204, 122 Stat. 3560, 3561-62 (Sept. 26, 2008). The amendments did not decriminalize this conduct.

COUNT 2
Aggravated Identity Theft
18 U.S.C. §§ 1028A(a)(1) and 2

13. The Grand Jury realleges and incorporates by reference the allegations in paragraphs 1-12 of this Indictment and charges that:

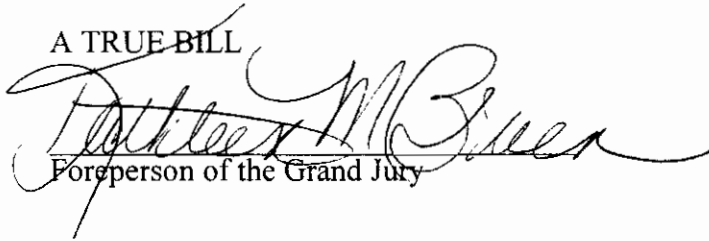
From approximately October 1, 2006 through February 7, 2007, in the District of Massachusetts and elsewhere, the defendant,

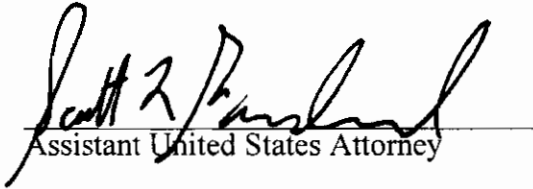
FRANCIS G. JANOSKO,

during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c) — that is, a violation of 18 U.S.C. § 1030(a)(5) — knowingly possessed, transferred, and used, without lawful authority, a means of identification of another person — that is, the names, birth dates, and Social Security numbers of current and former personnel of the Plymouth County Correctional Facility.

All in violation of 18 U.S.C. § 1028A(a)(1) and 2.

A TRUE BILL


Foreperson of the Grand Jury

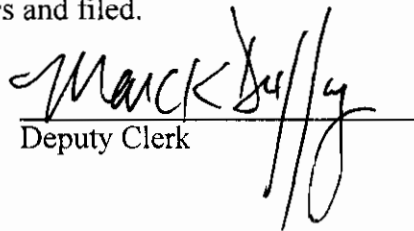

Assistant United States Attorney

DISTRICT OF MASSACHUSETTS

October 29, 2008

@ 2:35 pm

Returned into the District Court by the Grand Jurors and filed.


Deputy Clerk