United States District Court

EASTERN **DISTRICT OF** **MICHIGAN**

UNITED STATES OF AMERICA

V.

ADAM WILLIAM BOTBYL and
PAUL GREGORY TIMMINS,
defendants.

CRIMINAL COMPLAINT

CASE NUMBER: *03-81002*

I, the undersigned complainant being duly sworn state the following is true and correct to the best of my knowledge and belief: From on or about October 25, 2003, through on or about November 9, 2003, in Oakland County, in the Eastern District of Michigan, the defendants did, knowingly cause the transmission of a program, information, code and command and as a result of such conduct intentionally caused damage, without authorization, to a protected computer, in that they; without authority, accessed the computer network of "Lowe's" a company engaged in interstate commerce and by that unauthorized access caused damage by gaining access to stored data and impairing the integrity of the network; in violation of Title 18 United States Code, Section 1030(a)(5)(A)(i).

I further state that I am an agent with the Federal Bureau of Investigation and that this complaint is based on the following facts:

(PLEASE SEE ATTACHED AFFIDAVIT)

A TRUE COPY
CLERK, U.S. DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
BY _____ DEPUTY CLERK

Continued on the attached sheet and made a part hereof: ☒ Yes ☐ No

Signature of Complainant
Denise Stemen, Special Agent
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,

November 10, 2003
Date

at Detroit, Michigan
City and State

VIRGINIA M. MORGAN
United States Magistrate Judge
Name & Title of Judicial Officer

VIRGINIA M. MORGAN
Signature of Judicial Officer

AFFIDAVIT

I, Denise M. Stemen, being duly sworn hereby depose and state:

I. Introduction.

I am employed as a Special Agent of the Federal Bureau of Investigation ("FBI") and have been so employed since June of 1999. Since July of 2001, I have been assigned to investigate computer and high technology crimes. I have received training from the FBI regarding computer crimes and I have extensive experience regarding computers, computer networking, and the workings of the Internet. I have previously investigated violations of Title 18, United States Code, Section 1030, Fraud and Related Activity in Connection with Computers.

This affidavit is made in support of a complaint and arrest warrant for violations of Title 18, United States Code Section 1030(a)(5)(A)(i), Fraud and Related Activity in Connection with Computers.

The facts set forth below are based upon my own personal observations, reports and information provided to me by other law enforcement officials, and records I have obtained. I have been in communication with Special Agent Donald W. McArthur of the Charlotte, South Carolina Division of the FBI. SA McArthur told me he has been employed with the FBI since February of 1985 and since November of 1999, has been assigned to investigate computer and high technology crimes. SA McArthur received training from the FBI regarding computer crimes and has extensive experience with computers, computer networking, and the workings of the Internet. He has previously investigated violations of Title 18, United States Code, Section 1030, Fraud and Related Activity in Connection with Computers, and has served as affiant in numerous complaints and search warrants executed in the investigation of computer crimes.

This affidavit is intended to show that there is probable cause for this complaint.

II. Statement of Probable Cause.

SA McArthur advised me that he has been involved in the investigation of an unauthorized access of computers and computer networks belonging to Lowe's Corporation. These computers are used in the management of the Lowe's Home Improvement Stores in general, and in the processing of credit card purchases at those stores in particular. As such, the computers of Lowe's Corporation are "protected computers" as defined under Title 18, United States Code Section 1030(e)(2)(B).

SA McArthur advised me that he has been working closely with the Lowe's Corporation Network Security and System Administration personnel at the Lowe's Corporation headquarters in North Wilkesboro, North Carolina. These Network Security and System Administration personnel have been tracking the actions of an intruder or intruders who have gained unauthorized access to the Lowe's computer network, copied, changed and altered computer programs on the Lowe's network, and issued commands on the network with the purpose of illegally intercepting credit card transaction details processed by the network.

SA McArthur advised me that his investigation and his interviews of the Lowe's Network Security and System Administration personnel have determined that on October 25, 2003, at approximately 11:20 p.m., Eastern Standard Time, an unknown individual or individuals gained access to the computer network of the Lowe's store located at 28650 Telegraph Road, Southfield, Michigan. Upon gaining unauthorized access to this network, the unknown individual(s) accessed computers within the Central Data Center (CDC) section of the computer network of Lowe's, located at Lowe's Corporate Headquarters, State Highway 268 East, North Wilkesboro, North Carolina. On at least seven subsequent occasions, from October 26, 2003 to November 5, 2003, the unknown individual(s) gained access to seven additional Lowe's store networks in the following locations: 1) Salina, Kansas, 2) Wilkesboro, North Carolina, 3) Long Beach, California (two separate occasions), 4) Visalia, California, 5) Louisville, Kentucky, and 6) Rapid City, South Dakota. In total, as of 11:59 p.m. on November 6, 2003, seven Lowe's store computer networks and the CDC at the Lowe's corporate headquarters were accessed without authority on at least eight occasions. On November 5, 2003, the unknown individual(s), installed a malicious program on the Lowe's store computer network in Long Beach, California, which resulted in several computers, including point-of-sale computers, being disabled. Within the Lowe's network, the unknown individual(s) also accessed 12 accounts receivable signature files.

SA McArthur told me that investigation by the network security staff of Lowe's determined that the intruder(s) was accessing their network by logging onto a user account via the wireless network segment of the Lowe's store in Southfield, Michigan. Based upon my training and experience, and on the training and experience of SA McArthur, I know that computer networks often utilize Wireless Access Points to allow radio connections from portable computers and computing devices to traditional computer networks.

SA McArthur advised me that once logged onto the network, the intruder(s) was accessing computers throughout the Lowe's network. An examination of the wireless access points of the Lowe's store in Southfield, Michigan, indicated that the accesses were most likely being conducted within 1,000 feet of the store.

SA McArthur told me that on the morning of November 7, 2003, the network security staff of Lowe's detected an unauthorized access to the wireless network at the Lowe's store in Southfield, Michigan. I went with a FBI surveillance team to the Southfield, Michigan location at that time. The network security staff of Lowe's monitored the activities of the intruder(s) and observed the intruder preparing remote access and penetration programs and deploying them on the computers of the Lowe's store located in Gainesville, Florida. The intruder(s) then disconnected from the Southfield, Michigan wireless network before the surveillance team was in place.

At approximately 8:35 P.M. November 7, 2003, the FBI surveillance team, of which I was part, conducted surveillance at the Lowe's store parking lot in Southfield, Michigan. During that surveillance we observed two white males parked in a white Pontiac Grand Prix, Michigan License, TVW-638, sitting in the Lowe's lot. Theh passenger of the the car was seen using a laptop. A search of Michigan Secretary of State for the license plate, TVW-638, identified the registered owner of the 1995 Pontiac as ADAM WILLIAM BOTBYL, 2842 Oak Court, Spring Lake, Michigan, date of birth 07-26-1983, white male, 6'5", 275 lbs., brown hair, brown eyes.

FBI surveillance team continued to monitor the white Pontiac Grand Prix and the two occupants. At approximately 8:55 P.M., SA Jason L. Nestelroad of the FBI surveillance team went, on foot, to the Lowe's parking lot where the Pontiac Grand Prix was parked in an attempt to see the lap top screen located on the passenger's lap. As SA Nestelroad approached the Pontiac, the headlights were turned on and the car pulled out of the Lowe's parking lot. SA Chris Allen of the FBI surveillance team followed the Pontiac Grand Prix from the Lowe's parking lot onto Telegraph Road, northbound. SA Allen followed, the Grand Prix to the Rainbow Plaza, Little Caesar's Pizza, located at Telegraph Road. Both white males got out of the car and entered the pizzeria, ordered take-out, and got back into their car. SA Allen followed the Pontiac Grand Prix and the two white males to the Waterford Cinema 16, 7501 Highland Road (M-59), Waterford Township, Michigan. Both white males got out of the car and entered the cinema and went past the ticket taker. SA Allen described the driver of the Grand Prix as a white male, 6'3", 225 to 250 lbs. medium brown hair, glasses, beard, approximately twenty-five years of age. The passenger was described as approximately the same height as the driver, 200 lbs, long side burns, with brown hair.

SA Allen went to the Pontiac Grand Prix, Michigan license TVW-638, parked in the Waterford Cinema 16 parking lot to visually inspect it for exterior antennas and the laptop seen by the FBI surveillance team. SA Allen saw two exterior antennas on the Pontiac. On the rear of the roof on the driver's side, SA Allen saw a four inch high, chrome antenna with a four inch in diameter base, possibly magnetic. The second antenna displayed the label, "Terk Sirius Satellite Radio." SA Allen also saw a laptop laying on the backseat of the Pontiac and what appeared to be second laptop on the floor behind the driver's seat.

SA McArthur told me that on the evening of November 7, 2003, and extending through the early morning of November 8, 2003, the Network Security personnel of Lowe's conducted an extensive examination of network log files, software and user accounts, and determined that the intruder(s) accessing the wireless network at the Lowe's at Southfield, Michigan had altered and compromised the software utilized by Lowe's to process credit card purchases throughout the nation. These same personnel also determined that software alterations resulted in the capture of the credit card details of at least six Lowe's customers. Lowe's Network Security personnel determined that the intruder gained unauthorized access to the Lowe's network at approximately 8:42 P.M. This unauthorized access co-insides with the FBI surveillance of the Pontiac Grand Prix, Michigan license, TVW-638, in the Lowe's parking lot in Southfield, Michigan.

Through the Michigan Secretary of State, I asked for a copy the Michigan Driver License of, ADAM WILLIAM BOTBYL, date of birth 07/26/1983, Michigan Drivers license number B314031887587, who was the registered owner of the Pontiac Grand Prix. On 11/08/2003, SA Allen positively identified the driver of the Pontiac Grand Prix he followed to the Waterford 16 cinema, as the same person who appeared on the digital image provided by the Michigan Secretary of State for ADAM WILLIAM BOTBYL.

On 11/08/2003, a CHOICEPOINT search was conducted on ADAM WILLIAM BOTBYL, date of birth 07/26/1983 which yielded a previous address for BOTBYL as 930 VILLAGE GREEN LANE, APARTMENT 2014, Waterford, Michigan. At approximately 5:00 P.M. SA Allen identified the Pontiac Grand Prix, Michigan License plate TVW-638, sitting in the parking lot of the apartment complex. At approximately 5:40 P.M., SA Allen observed BOTBYL and the same white male (UNSUB 1) that SA Allen had observed the night before, at that location.

At approximately 9:02 P.M. on November 8, 2003, the FBI Surveillance team was in the parking lot of the Lowe's store at 28650 Telegraph Road, Southfield, Michigan and saw the Pontiac Grand Prix enter the parking lot and stop at a spot northwest of the main entrance to Lowe's. At that time I was on foot, walked passed the rear of the vehicle and saw UNSUB 1 operating a laptop computer at the command prompt with several windows open. BOTBYL was pulling out a laptop and activating it. BOTBYL and UNSUB 1 continued to work on the laptops for approximately 10 minutes when they moved the car south in the parking lot, repositioning it closer to the indoor lumber entrance. At approximately 9:25 P.M., they left the Lowe's parking lot and FBI surveillance followed them to, 930 VILLAGE GREEN LANE, Waterford, Michigan.

Subsequently, SA Allen reported a number of vehicle license plate numbers parked in the direct vicinity of the Pontiac Grand Prix. One of the vehicle plates, KC8-QAY, 2000 GMC Jimmy, came back to PAUL GREGORY TIMMINS, 930 VILLAGE GREEN LANE, APARTMENT 2014, Waterford, Michigan. The Michigan Secretary of State records describe TIMMINS as a white male, date of birth 01/01/1981, 6'2", 220 lbs., hazel eyes, corrective lens. This address matches BOTBYL's previous address and the location of the Pontiac Grand Prix. The physical description given by SA Allen matches that of TIMMINS.

I requested a digital image of the registered owner of the GMC Jimmy, PAUL GREGORY TIMMINS, date of birth 01/01/1981, Michigan Drivers license number T552676288002 from the Michigan Secretary of State, which I received. I positively identified the passenger of the Pontiac Grand Prix as the same person who appeared in the digital image provided by the Michigan Secretary of State for PAUL GREGORY TIMMINS.

Based upon the information detailed in this affidavit, and upon my training and experience, I believe there is probable cause that ADAM WILLIAM BOTBYL and PAUL GREGORY TIMMINS where engaged in conduct that constitutes a violation of Title 18, United States Code, Section 1030(a)(5)(A)(i), Fraud and Related Activity in Connection with Computers.

Denise M. Stemen
Special Agent Federal Bureau of Investigation

SWORN AND SUBSCRIBED TO
BEFORE ME THIS 10th DAY OF
NOVEMBER, 2003

VIRGINIA M. MORGAN

VIRGINIA M. MORGAN
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF MICHIGAN