

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	CRIMINAL NO. 19-CR-00081 (RMC)
	:	
v.	:	
	:	
SONAL PATEL,	:	
	:	
Defendant.	:	

FILED
APR - 4 2019
Clerk, U.S. District and
Bankruptcy Courts

STATEMENT OF OFFENSE

The United States of America, by the undersigned attorneys, the United States Attorney for the District of Columbia, and the Acting Chief of the Criminal Division’s Public Integrity Section, respectfully submit the following Statement of Offense in the above-captioned matter.

The following proffer of the government’s evidence is intended only to provide the Court with enough evidence to satisfy the mandate of Rule 11(b)(3) of the Federal Rules of Criminal Procedure. This proffer is not intended to be a disclosure of all the evidence available to the United States nor, to the extent it makes representations concerning anything the defendant said, is it a recitation of all that the defendant said.

Had this matter gone to trial, the government’s evidence would have shown, beyond a reasonable doubt, the following facts.

Introduction

1. The defendant SONAL PATEL worked as a Branch Chief within the Information Technology Division of the U.S. Department of Homeland Security-Office of Inspector General (“DHS-OIG”), located at 1120 Vermont Avenue, N.W., in Washington D.C. The defendant oversaw the development and maintenance of DHS-OIG’s Enforcement Database System

(“EDS”). Prior to joining DHS-OIG in February 2009, the defendant worked at the Transportation Security Administration (“TSA”) and the U.S. Postal Service-Office of Inspector General (“USPS-OIG”). While at USPS-OIG, the defendant worked on USPS-OIG’s case management systems, including USPS-OIG’s STARS database, which was used primarily for investigations and audits, as well as USPS-OIG’s PARIS applications, which USPS-OIG employees used to interface with the STARS database. While at DHS-OIG, the defendant did not request or receive any authorizations for outside employment.

2. Co-Conspirator 1 founded Delta Business Solutions, Inc., a Maryland corporation, in September 2015. Co-Conspirator 1 worked for DHS-OIG from February 2008 until 2013, including as DHS-OIG’s Acting Inspector General. While at DHS-OIG, Co-Conspirator 1 supervised the defendant, both directly and indirectly. Prior to working at DHS-OIG, Co-Conspirator 1 worked at TSA and USPS-OIG. Co-Conspirator 1 began supervising the defendant at USPS-OIG when Co-Conspirator 1 was the Director of Information Technology and the Deputy Chief Information Officer.

3. Co-Conspirator 2 worked as an Information Technology (“IT”) Specialist within the Information Technology Division of DHS-OIG and was supervised by the defendant. Prior to joining DHS-OIG in June 2010, Co-Conspirator 2 worked at USPS-OIG.

The Conspiracy to Commit Theft of Government Property

4. EDS is the case management system used by the DHS-OIG Office of Investigations. In or about 2008, DHS obtained ownership rights to the EDS source code. Since 2008, DHS-OIG has substantially modified and enhanced the EDS system. The initial contract for the EDS system cost DHS approximately \$3,161,620.30. One substantial modification to EDS

was the creation of an “eSubpoena” module. The functional specifications for the module were finalized on or about September 29, 2014. The defendant oversaw the development and implementation of this module by government employees and government contractors working under her. These employees included Co-Conspirator 2, who was the principal developer on this module. As detailed below, the defendant used her position within DHS-OIG to access and create digital copies of (1) the EDS source code, which included the eSubpoena module, (2) DHS-OIG’s database, which included the personal identifying information (“PII”) of DHS employees, and (3) the PII of U.S. Postal Service (“USPS”) employees. The defendant did this over the course of several months for the purpose of providing this data to Co-Conspirator 1 so that he could develop a commercially-owned version of a case management system, referred to as “EDS 2.0,” that could in turn be offered for sale to government agencies.

5. In 2009, Co-Conspirator 1 provided the defendant with a CD containing USPS-OIG’s STARS database, source code, scripts, and file server contents, which included the PII of USPS employees. Co-Conspirator 1 had the defendant copy the contents of the CD to the DHS-OIG server to enhance DHS-OIG’s audit systems.

6. On October 14, 2014, the defendant copied the EDS source code, which included the eSubpoena module, and database files from the DHS-OIG computer network onto an optical disk.

7. On or about November 4, 2014, the defendant instructed a subordinate DHS-OIG employee to send the defendant instructions on how to install the EDS system. Pursuant to the defendant’s request, the DHS-OIG employee provided the defendant with instructions on how to rebuild the EDS system on an alternate server.

8. On or about November 4, 2015, the defendant sent, from her personal Yahoo! email account to Co-Conspirator 1's Verizon email account, a list of Multiple Activation Keys and a Key Management Services Code associated with various Microsoft software products. These Multiple Activation Keys and Key Management Services Code, which could be used to download Microsoft software products without payment, being the property of DHS-OIG and the United States Government, had a value of approximately \$348,362.00.

9. On or about December 1, 2015, an employee at the U.S. Department of Agriculture-Office of Inspector General ("USDA-OIG") emailed the defendant to inquire about acquiring EDS from DHS-OIG for USDA-OIG. USDA-OIG would have been able to obtain EDS from DHS-OIG free of charge based on a Memorandum of Understanding between the agencies. Several months later, the defendant called the USDA-OIG employee and stated that she thought that USDA would be better served by EDS 2.0, a commercial product being developed by Co-Conspirator 1, with the defendant's assistance, and Co-Conspirator 2. The defendant further stated that she and Co-Conspirator 1 would like to meet with the USDA-OIG employee to discuss EDS 2.0.

10. On or about May 25, 2016, the defendant sent, from her personal Yahoo! email account to Co-Conspirator 1's Verizon email account, a list of the key benefits of EDS 2.0.

11. On or about May 26, 2016, the defendant and Co-Conspirator 1 met with the USDA-OIG employee at a restaurant in the District of Columbia. At that meeting, the defendant and Co-Conspirator 1 discussed the benefits of EDS 2.0 and the disadvantages of DHS-OIG's EDS. The USDA-OIG employee expressed interest in the eSubpoena module that was present in DHS-OIG's EDS. The defendant stated that she could "tell him [Co-Conspirator 1] the concepts" of eSubpoena so that Co-Conspirator 1 could incorporate eSubpoena into EDS 2.0. The defendant

further stated that Co-Conspirator 2 could incorporate eSubpoena into EDS 2.0. Co-Conspirator 1 stated that he would give the defendant his input so that the costs for USDA-OIG to purchase EDS 2.0 could be developed.

12. On or about May 27, 2016, the defendant copied DHS-OIG's EDS source code and database from the DHS-OIG computer network onto optical disks in order to provide them to Co-Conspirator 1 to aid in his development of EDS 2.0. On or about May 27, 2016, the defendant also sent, from her government email account to her personal Yahoo! email account, a government document containing detailed instructions for rebuilding the EDS web applications from backup files onto another server. Also on May 27, 2016, the defendant forwarded that document from her Yahoo! email account to Co-Conspirator 1's Verizon email account.

13. On or about May 30, 2016, the defendant, Co-Conspirator 1, and Co-Conspirator 2 met at the defendant's residence in Sterling, Virginia. During the meeting, the defendant and Co-Conspirator 2 showed Co-Conspirator 1 improvements to the EDS system, including the addition of the eSubpoena module. The defendant, Co-Conspirator 1, and Co-Conspirator 2 discussed technology for EDS 2.0 based on USPS-OIG's case management system and EDS.

14. In or about June 2016, the defendant met Co-Conspirator 1 on the side of the road in Virginia as Co-Conspirator 1 was on the way to Washington Dulles International Airport to travel to India to meet with software developers for the purpose of developing EDS 2.0. The defendant provided to Co-Conspirator 1 two DVDs containing DHS-OIG's EDS source code and data. Co-Conspirator 1 subsequently stored the EDS source code and database files on a server in his residence.

15. On or about June 27, 2016, Co-Conspirator 2 sent, from his government email account to the defendant's government email account, technical instructions relating to the EDS system. The defendant then sent these instructions from her government email account to her personal Yahoo! email account and then forwarded those instructions from her Yahoo! email account to Co-Conspirator 1's Verizon email account.

16. On or about June 30, 2016, the defendant and Co-Conspirator 1 participated in an online meeting with an Indian-based software development company, with which Co-Conspirator 1 and Delta Business Solutions, Inc. had contracted for services associated with developing EDS 2.0. Co-Conspirator 1 provided software developers with the Indian company remote access over the Internet to the EDS source code and DHS-OIG database files that the defendant had provided to Co-Conspirator 1 and that Co-conspirator 1 had saved on a non-government server.

17. On or about July 8, 2016, at the defendant's request, Co-Conspirator 2 sent, from his government email account to the defendant's government email account, a government document containing the functional requirements for the eSubpoena module. Also on or about July 8, 2016 and then again on or about July 20, 2016, the defendant sent that document from her government account to her personal Yahoo! email account. On or about July 8, 2016, the defendant forwarded that email and document from her personal Yahoo! email account to Co-Conspirator 1's Verizon email account.

18. In or about July 2016, Co-Conspirator 1 provided a laptop computer to the defendant. The defendant brought the laptop computer to DHS-OIG headquarters and delivered it to Co-Conspirator 2. On or about July 13, 2016, the defendant requested that Co-Conspirator 2 check the laptop computer to determine whether fresh downloads of DHS-OIG's EDS source code

and database files were needed, or whether the laptop computer just needed to be configured. Co-Conspirator 2 subsequently delivered the laptop computer to the Co-Conspirator 1 at a location in Virginia.

19. On or about November 2, 2016, the defendant sent, from her personal Yahoo! email account to Co-Conspirator 1's Verizon email account, U.S. General Services Administration public information on pricing case management systems for the defendant and Co-Conspirator 1 to use as a basis for pricing EDS 2.0.

20. In or about February 2017, Co-Conspirator 1 could not find his copy of the CD containing the USPS-OIG database, EDS source code, scripts, and file server contents. Co-Conspirator 1 wanted to put these items onto a computer server in his home where he could work on developing the software system. To assist Co-Conspirator 1 in this respect, the defendant once again copied the USPS-OIG database, source code, scripts, and file server contents from the DHS-OIG server onto an optical disk. On or about March 21, 2017, the defendant provided two DVDs containing these items to Co-Conspirator 2 for delivery to Co-Conspirator 1. Co-Conspirator 2 met Co-Conspirator 1 outside of DHS-OIG headquarters in Washington, D.C., and delivered the DVDs to Co-Conspirator 1.

21. In or about March 2017, the defendant and Co-Conspirator 1 participated in an online meeting with an Indian-based software development company during which employees of the Indian-based software development company demonstrated what they had produced.

22. On April 19, 2017, law enforcement executed search warrants at the defendant's residence in Sterling, Virginia, and Co-Conspirator 1's residence in Sandy Spring, Maryland. From Co-Conspirator 1's residence, law enforcement recovered multiple laptop computers,

computer servers, optical devices (CDs and DVDs), and external data storage drives (USB drives). On the computer server, law enforcement located a copy of DHS-OIG's EDS system, including, but not limited to, the following information: information on 158,924 DHS-OIG investigative cases through December 18, 2014; entries for 36,824 witnesses, subjects, victims, and other individuals associated with DHS-OIG cases; and PII for 189,376 DHS employees, including names, dates of birth, social security numbers, addresses, and pay grades. All of this data constituted government property that the defendant knowingly provided to Co-Conspirator 1 to assist him in the development of EDS 2.0. Forensic analysis further revealed that the server in Co-Conspirator 1's residence contained a version of USPS-OIG's case management system and the PII of USPS employees, both of which also constituted government property that the defendant provided to Co-Conspirator 1 to assist him in the development of EDS 2.0.

23. During the search at Co-Conspirator 1's residence, law enforcement also recovered numerous optical disks containing DHS-OIG's EDS source code and database files which the defendant had provided to Co-Conspirator 1, including the files which the defendant had copied from the DHS-OIG computer network on or about October 14, 2014.

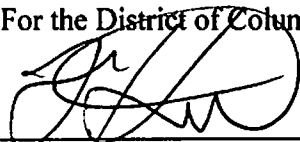
24. In total, law enforcement determined that the defendant, Co-Conspirator 1, and Co-Conspirator 2 obtained the PII of approximately 246,167 DHS employees and 6,723 USPS employees. In order to address the potential effects of the conduct of the defendant, Co-Conspirator 1, and Co-Conspirator 2, DHS spent approximately \$448,023.94 on an initial contract to provide credit monitoring and notification services for affected individuals. USPS spent approximately \$33,148.84 to provide credit monitoring and notification services for affected individuals.

Limited Nature of Proffer

25. This proffer of evidence is not intended to constitute a complete statement of all facts known by the defendant, but is a minimum statement of facts intended to provide the necessary factual predicate for the guilty plea. The limited purpose of this proffer is to demonstrate that there exists a sufficient legal basis for defendant's plea of guilty to the charged crime.

JESSIE K. LIU
UNITED STATES ATTORNEY
For the District of Columbia

By:

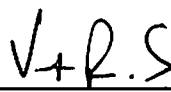


DAVID B. KENT
D.C. Bar No. 482850
Assistant United States Attorney
555 4th Street, N.W.
Washington, D.C. 20530
(202) 272-7762
David.Kent@usdoj.gov

Respectfully submitted,

ANNALOU TIROL
ACTING CHIEF
Public Integrity Section

By:



VICTOR R. SALGADO
D.C. Bar No. 975013
Trial Attorney
Public Integrity Section, Criminal Division
1400 New York Avenue, N.W.
Washington, D.C. 20005
(202) 353-4580
Victor.Salgado@usdoj.gov

DATED: January 10, 2019

DEFENDANT'S ACCEPTANCE

The preceding statement is a summary, made for the purpose of providing the Court with a factual basis for my guilty plea to the charges against me. It does not include all of the facts known to me regarding this offense. I make this statement knowingly and voluntarily and because I am, in fact, guilty of the crime charged. No threats have been made to me nor am I under the influence of anything that could impede my ability to understand this Statement of Offense fully.

I have read every word of this Statement of the Offense, or have had it read to me. Pursuant to Federal Rule of Criminal Procedure 11, after consulting with my attorney, I agree and stipulate to this Statement of the Offense, and declare under penalty of perjury that it is true and correct.

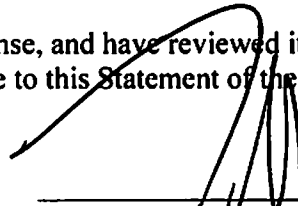
Date: 04/04/2019

Sonal Patel
SONAL PATEL
Defendant

ATTORNEY'S ACKNOWLEDGMENT

I have read this Statement of Offense, and have reviewed it with my client fully. I concur in my client's desire to adopt and stipulate to this Statement of the Offense as true and accurate.

Date: Apr 1 4, 2019



THOMAS C. HILL, Esq.
Counsel for Defendant Patel