

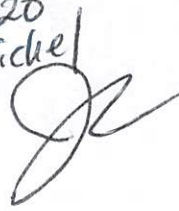
UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF LOUISIANA

UNITED STATES OF AMERICA	*	CRIMINAL NO. 19-230
v.	*	SECTION: "A"
COLBI TRENT DEFIORE	*	

\* \* \*

FACTUAL BASIS


U.S. DISTRICT COURT  
EASTERN DISTRICT OF LOUISIANA  
FILED 1-7-2020  
Carol L. Michel  
CLERK



The defendant, **COLBI TRENT DEFIORE**, (hereinafter, the “defendant” or “DEFIORE”), has agreed to plead guilty as charged to the Indictment now pending against him, charging him with intentionally accessing a protected computer in excess of authorization for private financial gain and in furtherance of criminal act, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B)(i), and (c)(2)(B)(ii). Both the Government and the defendant, **COLBI TRENT DEFIORE**, do hereby stipulate and agree that the following facts set forth a sufficient factual basis for the crimes to which the defendant is pleading guilty. The Government and the defendant further stipulate that the Government would have proven, through the introduction of competent testimony and admissible, tangible exhibits, the following facts, beyond a reasonable doubt, to support the allegations in the Indictment now pending against the defendant:

The Government would establish that Company A was a Virginia-based company in the technology sector. Company A supported the Centers for Medicare & Medicaid Services (CMS) by operating contact centers to assist with, among other things, Medicare enrollment. One of these contact centers was located in Bogalusa, Louisiana (the Bogalusa Contact Center (BCC)), within the Eastern District of Louisiana.

Fee \_\_\_\_\_  
Process \_\_\_\_\_  
X Dktd \_\_\_\_\_  
CtRmDep \_\_\_\_\_  
Doc. No \_\_\_\_\_



AUSA JG  
Defendant CM  
Defense Counsel VWJ

The Government would further establish that Company A often hired temporary employees on a seasonal basis to support peak call volumes associated with annual enrollments. Company A hired **DEFIORE** to work at the BCC as a Customer Service Representative (CSR) on a seasonal basis on three separate occasions: August 29, 2014 to November 23, 2014; July 31, 2017 to February 3, 2018; and September 10, 2018 to November 16, 2018. In his capacity as a CSR, **DEFIORE**'s responsibilities included assisting consumers with enrolling under the Affordable Care Act and answering questions posed by consumers via phone. As a CSR, **DEFIORE** had access to the healthcare.gov database, which contained various personally identifiable information (PII) of consumers. Accessing the healthcare.gov database and its contents was made possible through the use of a "protected computer," as that term is defined by Title 18, United States Code, Section 1030(e)(2).

The Government would further establish that Company A provided a limited number of employees with the ability to access certain portions of Company A's network, including their work email accounts, remotely via a multi-factor authentication process. Employees authorized to access Company A's network remotely received a software token to facilitate their remote access.

The Government would further establish that during the course of employment and prior to obtaining access to consumers' PII, Company A's employees, including **DEFIORE**, underwent training on a variety of subjects, including how to handle consumers' PII. During the training, Company A provided **DEFIORE** the following pertinent information: employees were to minimize their reproduction or exposure to consumer PII data; employees were only allowed to transmit PII data electronically to the extent required by business requirements; any electronic

transmission containing PII had to be encrypted; only authorized devices were permitted to access systems hosting consumer PII data; and bulk searches of the healthcare.gov database for consumers and their data was prohibited.

The Government would further establish that beginning at a time unknown, but not later than October 31, 2018, and continuing until at least November 12, 2018, **DEFIORE** improperly accessed and obtained, without authorization, the PII data of more than 8,000 individuals through his improper usage of the healthcare.gov database. **DEFIORE** did so for the purpose of his private financial gain and in furtherance of criminal acts, including wire fraud, in violation of Title 18, United States Code, Section 1343. Thereafter, **DEFIORE** then used the PII data he improperly obtained to apply for credit and financial benefits, including an automobile loan and cards.

The Government would further establish that **DEFIORE** exceeded his authorized access to Company A's network and the healthcare.gov database and obtained the PII data of consumers illicitly in the following way. First, **DEFIORE** conducted a series of bulk searches of the healthcare.gov database based on first and last names. Each bulk search returned PII for numerous consumers, including names, dates of birth, social security account numbers, addresses, emails, gender, and user names. The bulk searches were unrelated to the customer(s) **DEFIORE** was supporting in his capacity as CSR. Thereafter, **DEFIORE** highlighted the search results and copied the PII data onto a virtual clipboard. Next, while on duty at BCC, **DEFIORE** copied the PII data from the virtual clipboard and pasted it into one or more emails using his internal work email account: colbi.defiore@[Company A].com. **DEFIORE** then sent the emails containing PII data to his work email account at colbi.defiore@[Company A].com. After work hours, **DEFIORE** accessed Company A's network remotely without authorization to retrieve his work email.

**DEFIORE** saved the PII data he obtained improperly in several ways, including by handwriting the information in notebooks and sending screenshots of his work emails that contained PII to his personal email account: defioretcolbi@gmail.com. **DEFIORE** used the PII of at least five (5) consumers he obtained to apply fraudulently for at least six (6) credit cards, loans, and lines of credit for his personal benefit. **DEFIORE** submitted at least one of the applications online, which caused the transmission of a wire communication to travel interstate.

The Government would further establish that **DEFIORE** engaged in the unauthorized conduct described above on multiple dates, including November 6, 2018, November 7, 2018, November 8, 2018, and November 12, 2018.

The Government would further establish, through the testimony of Federal Bureau of Investigation Special Agent Timothy Yee, that on or about February 15, 2019, the Federal Bureau of Investigation executed a search warrant authorized by a United States Magistrate Judge sitting in the Southern District of Mississippi at **DEFIORE**'s residence, 44 Albert Prince Road, Carriere, Mississippi. Law enforcement authorities seized multiple electronic devices and hand-written documents belonging to **DEFIORE**, including his personal home iMac computer. Subsequent review of the information revealed that the devices and documents contained evidence that **DEFIORE** had obtained PII data from Company A. Law enforcement authorities also seized notebooks into which **DEFIORE** copied consumers' PII data.


The Government would further establish, through the introduction of documentary evidence and the testimony of representatives of Company A, that by engaging in the actions described above, **DEFIORE** caused Company A to suffer reasonably foreseeable loss, specifically

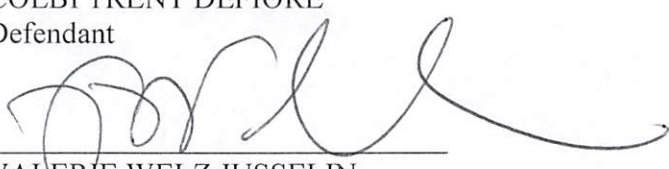
costs associated with responding to **DEFIORE'S** offense, conducting a damage assessment, responding to and remediating damage, contacting consumers who were potential victims, and providing theft protection services for them.

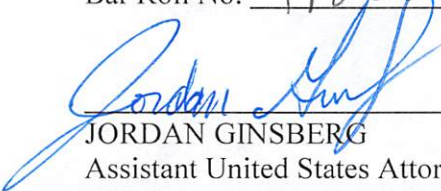
The above facts originate from an investigation conducted by, and would be proven at trial by credible testimony from, Special Agents from the Federal Bureau of Investigation, representatives of Company A, and documents and tangible exhibits in the custody of the Federal Bureau of Investigation, and the statements of the defendant, **COLBI TRENT DEFIORE**.

**Limited Nature of Factual Basis**

This proffer of evidence is not intended to constitute a complete statement of all facts known by **DEFENDANT** and/or the Government. Rather, it is a minimum statement of facts intended to prove the necessary factual predicate for his guilty plea. The limited purpose of this proffer is to demonstrate that there exists a sufficient legal basis for the plea of guilty to the charged offense by **DEFENDANT**.

  
COLBI TRENT DEFIORE  
Defendant

  
VALERIE WELZ JUSSELIN  
Attorney for Defendant Defiore  
Bar Roll No. 19825

  
JORDAN GINSBERG  
Assistant United States Attorney  
Illinois Bar Roll No. 6282956