UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon. Michael A. Hammer
	:	
v.	:	Mag. No. 21-10413
	:	
JONATHAN KATZ	:	**CRIMINAL COMPLAINT**

I, Molly E. Pyatt, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this Complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.

Molly E. Pyatt

Molly E. Pyatt, Special Agent
Federal Bureau of Investigation

Attested to me by telephone pursuant to Fed. R. Crim. P. 4.1(b)(2)(A) on December 6, 2021, in the District of New Jersey.

HONORABLE MICHAEL A. HAMMER
UNITED STATES MAGISTRATE JUDGE

s/Hon. Michael A. Hammer /mr
Signature of Judicial Officer

Signed by Special Agent Pyatt at Judge Hammer's direction pursuant to F.R.C.P. 4.1(b)(6)(C).

ATTACHMENT A

COUNTS 1 THROUGH 5
(Unauthorized Access to a Protected Computer)

On or about the dates listed below, with each unauthorized access being a separate count, in the District of New Jersey and elsewhere, the defendant

JONATHAN KATZ

intentionally accessed a protected computer, specifically user accounts on the computer systems of Company-1, without authorization, and by means of such conduct obtained information from such protected computer.

Count	Date of Unauthorized Access	Victim
1	May 11, 2021	Victim 1
2	May 12, 2021	Victim 2
3	May 18, 2021	Victim 3
4	May 19, 2021	Victim 4
5	May 19, 2021	Victim 5

In violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B).

ATTACHMENT B

I, Molly Pyatt, being first duly sworn, depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Department of Justice, Federal Bureau of Investigation ("FBI"), and have been so employed since 2020. I am currently assigned to the Newark, New Jersey Field Office. My experience as an FBI Special Agent has included the investigation of cases involving fraud. I have received training and have gained experience in interview and interrogation techniques, arrest procedures, computer crimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. The information contained in this Affidavit is based upon my training and experience, conversations with other law enforcement officers, and review of documents and records.

2. Because this affidavit is being submitted for the limited purpose of establishing probable cause, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause. Unless specifically indicated, all dates, locations, quantities, and dollar amounts described in this affidavit are approximate, and all conversations and statements described in this affidavit are related in substance and in part.

BACKGROUND

3. At all times relevant to this Complaint:

a. Company-1 was a telecommunications company, with offices in New Jersey, that provided wireless telephone service in the United States and elsewhere;

b. Defendant Jonathan Katz ("KATZ") was a resident of New Jersey and was employed as a Manager by Company-1 at a location in New Jersey;

c. As a Manager at Company-1, KATZ had access to customer accounts and was able to modify, add, and make changes to such accounts, including swapping SIM numbers (as described below) at the customer's request;

d. Victim-1 was a Company-1 customer and a resident of Wyoming;

e. Victim-2 was a Company-1 customer and a resident of New Jersey;

f. Victim-3 was a Company-1 customer and a resident of

California;

g. Victim-4 was a Company-1 customer and a resident of Tennessee;

h. Victim-5 was a Company-1 customer and a resident of New Jersey.

i. In order to activate a mobile device for usage on cellular telephone networks, many devices are assigned a unique International Mobile Equipment Identity number ("IMEI") in combination with a unique subscriber identity module ("SIM"), encoded on a small removable chip or directly embedded into the device. This IMEI/SIM combination, when paired with a customer's mobile phone number assigned by a carrier, such as Company-1, is what allows a given user to authenticate a customer's subscription on a mobile phone carrier's network. This, in turn, allows the customer to make and receive cellular calls and text messages associated with the customer's mobile phone number.

j. Generally, "SIM Swapping" refers to a method of an unauthorized takeover of a victim's wireless account, carried out by linking a victim's mobile phone number to a SIM installed in a device controlled by the perpetrator of the swap. One method of conducting a SIM swap is with the assistance of an insider who has access to the provider's networks.

k. As a result of a SIM swap, phone calls and text messages sent to the victim's mobile phone number are routed to a device controlled by the attacker(s), giving the attacker complete control over the victim's mobile phone number. Upon gaining control of a victim's mobile phone number, an attacker can gain unauthorized access to victims' other electronic accounts—including email, social media, and cryptocurrency accounts—using various means, including intercepting "two-factor authentication" codes or resetting victims' passwords using information sent to the registered mobile phone number. Since the victims' physical cell phones are no longer tethered to their cell phone accounts, the victims do not receive account alerts or other indications that their online accounts have been compromised or accessed from unfamiliar devices.

PROBABLE CAUSE

4. On or about May 10, 2021, KATZ was contacted by an individual ("Individual-1") who ultimately offered KATZ $1,000 per swap to use KATZ's access to Company-1's computer network to perform SIM swaps.

5. Following these communications with Individual-1, KATZ agreed to conduct SIM swaps on several Company-1 accounts that Individual-1 provided to KATZ. KATZ used his managerial credentials to access Company-1's computer network to conduct unauthorized SIM swamps, as follows:

Count	Date of Unauthorized Access	Victim
1	May 11, 2021	Victim 1
2	May 12, 2021	Victim 2
3	May 18, 2021	Victim 3
4	May 19, 2021	Victim 4
5	May 19, 2021	Victim 5

6. Specifically, KATZ used his managerial access to Company-1's computer network to "swap" the SIM associated with the victims' phone numbers for another SIM loaded into a mobile device controlled by Individual-1.

7. In exchange for perpetrating these SIM swaps, KATZ received payment in the form of Bitcoin through Crypto Currency Exchange-1. Law enforcement obtained records from Crypto Currency Exchange-1 showing that KATZ received the above-described payments into his account on or about May 12, 2021, May 14, 2021, and May 19, 2021. The Crypto Currency Exchange-1 account was linked to KATZ through KATZ's photograph, social security number, and his New Jersey driver's license.

8. Company-1 confirmed that KATZ was not authorized to conduct the above-described SIM swaps.