UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	**CRIMINAL COMPLAINT**
	:	
v.	:	Honorable Jessica S. Allen
	:	
ERIC LEYKIN	:	Mag. No. 22-8277
	:	
	:	**FILED UNDER SEAL**

I, Joseph Landers, 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

/s/ Joseph Landers/AMT

Joseph Landers
Special Agent
Federal Bureau of Investigation
Special Agent Joseph Landers attested to this Affidavit by telephone pursuant to FRCP 4.1(b)(2)(A).

Sworn to before me telephonically
on August 9, 2022

/s/ Jessica S. Allen/AMT

Honorable Jessica S. Allen
United States Magistrate Judge

Signature of Judicial Officer

ATTACHMENT A

COUNT 1
(Wire Fraud – 18 U.S.C. § 1343)

From at least as early as in or about June 2022 through at least as recently as in or about July 2022, in the District of New Jersey and elsewhere, the defendant,

ERIC LEYKIN,

did knowingly and intentionally devise and intend to devise a scheme and artifice to defraud victims of money and property by means of false or fraudulent pretenses, representations, and promises, and on or about June 30, 2022, in Union County, in the District of New Jersey, and elsewhere, for the purpose of executing and attempting to execute this scheme and artifice to defraud, did knowingly transmit and cause to be transmitted by means of wire, radio, and television communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds.

In violation of Title 18, United States Code, Section 1343.

COUNT 2
(Computer Intrusion – 18 U.S.C. § 1030(a)(5)(B))

On or about July 1, 2022, in Essex County, in the District of New Jersey, and elsewhere, the defendant,

ERIC LEYKIN,

did intentionally access a protected computer without authorization, and as a result of such conduct, recklessly caused damage resulting in loss to one or more persons within a one-year period aggregating at least $5,000 in value.

In violation of Title 18, United States Code, Section 1030(a)(5)(B) and (c)(4)(A)(i)(I).

ATTACHMENT B

I, Joseph Landers, am a Special Agent with the Federal Bureau of Investigation (the "FBI"). I am fully familiar with the facts set forth herein based on my own investigation, my conversations with other law enforcement officers, and my review of reports, documents, and photographs of the evidence. Where statements of others are related herein, they are related in substance and part. Because this complaint is being submitted for a limited purpose, I have not set forth each and every fact that I know concerning this investigation. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

Background

1. At times relevant to this Complaint:

a. The defendant, Eric Leykin ("LEYKIN"), resided in Brooklyn, New York. He was the CEO of "Business-1," a clinical reference laboratory headquartered in Kenilworth, New Jersey.

b. The victim business, "Victim-1," was a clinical reference laboratory headquartered in Millburn, New Jersey. Business-1 was a competitor of Victim-1.

c. LEYKIN was the registered owner of a 2021 white BMW X5 bearing license plate HXU5892 (the "Leykin Vehicle").

d. "Network-1" was a major U.S. cellular service provider.

e. "Business-2" was a prepaid mobile device business. Business-2 sold both prepaid mobile devices and prepaid cellular minutes for use on those devices. Business-2 was owned by Network-1 and used Network-1's cellular network to conduct its operations.

f. "Retailer-1" was a major U.S. retail company.

g. "Vendor-1" was a technical services firm that Victim-1 used to service its laboratory equipment.

Overview of LEYKIN's Scheme

2. On or about July 1, 2022, LEYKIN gained access to Victim-1's laboratory premises under false pretenses. LEYKIN then proceeded to access Victim-1 computers without authorization and cause damage; steal Victim-1

computers and other devices and leave the Victim-1 premises with them; and cause significant damage to Victim-1 computers and other equipment.

Background to LEYKIN's July 1, 2022 Intrusion

3. Investigation has revealed that in or about January 2022, Victim-1 hired two former Business-1 employees, "Employee-1" and "Employee-2." Both of these employees are salespeople—they worked in sales at Business-1 and now work in sales at Victim-1. At the time of the July 1, 2022 incident, both employees were in the process of bringing former Business-1 clients to Victim-1. Law enforcement has learned from Victim-1, among other sources, that LEYKIN was upset by this development and had made threats to both Employee-1 and Employee-2 in an attempt to pressure them to return their clientele to Business-1. Victim-1 also reported having received, in the period leading up to the July 1, 2022 incident, strange phone calls from Google-provided phone numbers inquiring about Employee-1 and Employee-2.

4. Law enforcement has learned that on or about June 1, 2022, LEYKIN sent a cease-and-desist letter to Employee-1. In that letter, LEYKIN complained that Employee-1 was "attempting to interfere unlawfully with [Business-1's] business and contractual relationships with certain of its employees." LEYKIN also complained in that letter that "it has come to [Business-1's] attention that you have unlawfully solicited business from at least one of [Business-1's] clients." LEYKIN concluded that letter by warning Employee-1 that "[s]hould [Employee-1] not cease and desist from interfering with [Business-1's] business and contractual relationships and instead continue to cause [Business-1] harm, [Business-1] will have no option but to take all appropriate action to protect its interests. Please be guided accordingly."

5. Records obtained from Retailer-1 show that at or about 10:14 a.m. on June 30, 2022, a customer visited Retailer-1's store in Union, New Jersey, and paid cash to purchase: (1) a prepaid Business-2 mobile device (the "Prepaid Device") and (2) prepaid Business-2 cellular minutes for use on the Prepaid Device. Surveillance footage obtained from Retailer-1 at the point of sale for this transaction show the purchaser to be LEYKIN, as confirmed by comparing that footage with LEYKIN's New York driver's license records and other surveillance footage obtained in this investigation, discussed in more detail below.

6. Records and information obtained from both Victim-1 and Network-1 show that the Prepaid Device was activated shortly after being purchased by LEYKIN. Then, at or about 10:47 a.m. on that date—just over 30 minutes after LEYKIN bought the Prepaid Device—the Prepaid Device was used to place a call to a Victim-1 employee, during which the caller purported to be a Vendor-1 employee named "Scott." During that call, "Scott" scheduled an appointment with the Victim-1 employee to visit Victim-1 on the following day—July 1, 2022—between 4 p.m. and 6 p.m. to "service" Victim-1's laboratory equipment.

7. Records and information obtained from both Victim-1 and Network-1 show that the Prepaid Device was then used to place a second relevant call, at or about 2:02 p.m. on July 1, 2022, to the same Victim-1 employee. As with the June 30, 2022 call, the caller claimed to be a Vendor-1 employee named "Scott" and informed the Victim-1 employee that he was running late and would arrive at Victim-1 at 4:30 p.m.

LEYKIN's July 1, 2022 Intrusion

8. On or about July 1, 2022, law enforcement responded to Victim-1 on a report of theft and destruction of property. Upon arrival, Victim-1 employees reported to law enforcement that an individual named "Scott," claiming to be a technician with Vendor-1, had arrived at Victim-1 at or about 4:30 p.m. and had left sometime after about 5:00 p.m. Victim-1 employees reported that "Scott" had, among other things, inflicted significant damage on Victim-1's computer and laboratory equipment and had stolen hard drives within certain of those computers and laboratory equipment.

9. In particular, and among other things:

a. "Scott" had unplugged the backup generator in the rear of Victim-1's building.

b. "Scott" had removed at least four hard drives within Victim-1's servers. Those servers, Victim-1 informed law enforcement, connected to a resource called a "laboratory information system," which stores Victim-1's patient information, including patient's personally identifying information ("PII").

c. "Scott" also removed the hard drives of three other computers and rendered those computers inoperable.

d. "Scott" also tampered and/or cut other wiring inside Victim-1, including wiring connected to Victim-1's surveillance system.

10. Although "Scott" tampered with wiring connected to the surveillance system, Victim-1 was able to obtain and provide to law enforcement substantial surveillance footage showing "Scott's" activities, since the surveillance system was connected to a different server that "Scott" had not tampered with. The surveillance footage, captured from multiple camera angles, confirms what Victim-1 employees reported to law enforcement regarding "Scott's" activities. Among other things, the surveillance footage provides multiple clear angles of "Scott" that also matched Victim-1 employee descriptions: a white male around 5'9" in height, with distinctive long black hair tied in a bun and a face mark with facial hair visible around the mask, wearing a white Nike baseball hat,a blue shirt, blue jeans, Adidas sneakers, and a black North Face backpack.

11. In particular, the Victim-1 surveillance footage clearly shows "Scott" inserting a small object of about the size of USB thumb drive into the USB port of a computer. Within moments, the surveillance footage shows that computer's screen going blank, and "Scott" then removing that computer's hard drive. Further investigation has shown that computer to be completely destroyed and inoperable. Two other Victim-1 computers, also with their hard drives stolen, were found by law enforcement to be in the same condition.

12. Based on training, experience, and investigation—including review of this surveillance footage—law enforcement believes that the object "Scott" inserted into the USB port of this computer was a "USB kill stick." A USB kill stick is a device meant to destroy a targeted computer. Like other legitimate USB devices, a USB kill stick, once inserted, accesses a targeted computer and causes the computer to transmit power within USB design limits from the computer back into the kill stick—much as one might charge a mobile phone via a USB connection. Once the USB kill stick is fully charged in this way, however, it surges power back into the targeted computer far above design limits, destroying the computer. This process occurs within a few seconds of the USB kill stick being inserted. The damage found by law enforcement on both the computer discussed above and the other two computers is consistent with the use of a USB kill stick.

13. Victim-1 surveillance footage shows "Scott" entering Victim-1 on foot. Law enforcement, however, obtained surveillance footage captured by cameras close to the Victim-1 premises, including footage from one camera, "Camera-1," situated on a neighboring street to Victim-1 around three-tenths of a mile away from Victim-1. Camera-1's footage shows a white BMW X5—the same make, model, and color as the Leykin Vehicle—traveling toward Victim-1 at or about 4:19 p.m. on July 1, 2022, and a white BMW X5 traveling away from Victim-1 at or about 5:28 p.m. on the same date.

14. Victim-1 employees reported to law enforcement that they contacted Vendor-1 regarding the incident. Vendor-1 informed them that Victim-1 was not scheduled for any service on July 1, 2022 and that Vendor-1 did not employ any technician named "Scott."

15. This investigation has revealed that LEYKIN was "Scott." Among other things, both Employee-1 and Employee-2, who had worked with LEYKIN in the past, were each shown the Victim-1 surveillance footage, and both individuals represented to law enforcement that LEYKIN was the individual in the footage. Moreover, the individual in the surveillance footage closely matches other surveillance footage and images obtained by law enforcement in this investigation—including LEYKIN's New York State driver's license photo and the surveillance footage obtained from Retailer-1 in connection with the Prepaid Device. Finally, and as related above, a vehicle of the same make, model, and color as the Leykin Vehicle was captured on video both approaching and moving

away from Victim-1 at times consistent with the chronology of the July 1, 2022 incident, and the Leykin Vehicle itself was observed traveling back to Brooklyn at a time consistent with the chronology of the July 1, 2022 incident.

16. Business-2 has informed law enforcement that whenever either a Business-2 prepaid device is activated or Business-2 prepaid cellular minutes are redeemed, certain data is electronically transmitted from the point of sale to a Business-2 facility in Miami, Florida. Consequently, on or about June 30, 2022, when LEYKIN purchased the Prepaid Device and Business-2 prepaid cellular minutes at the Retailer-1 store in Union, New Jersey and then activated the Prepaid Device with those prepaid minutes, LEYKIN caused a wire transmission to be sent from New Jersey to Florida.