

United States District Court
District of New Jersey

UNITED STATES OF AMERICA : HON. MICHAEL A. HAMMER
v. : **CRIMINAL COMPLAINT**
RALPH MANDIL : Magistrate No. 16-4103
: Filed Under Seal

I, Anthony Czajkowski, the undersigned complainant 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 page and made a part hereof.



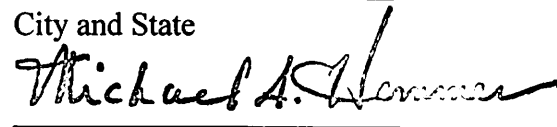
Anthony Czajkowski
Special Agent
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,

October 12, 2016 at
Date

Newark, New Jersey
City and State

Honorable Michael A. Hammer
United States Magistrate Judge



Signature of Judicial Officer

ATTACHMENT A

Count One
(Theft of Trade Secrets)

From in or about August 1, 2016 through in or about October 12, 2016 in Bergen County, in the District of New Jersey and elsewhere, defendant

RALPH MANDIL

did knowingly and intentionally attempt to steal, and without authorization appropriate, take, carry away, obtain by fraud and deception, copy, duplicate, download, upload, transmit, deliver, send, communicate or convey information with respect to trade secrets belonging to Victim 1 with intent to convert trade secrets related to and included in a product that is produced for and placed in interstate and foreign commerce, to the economic benefit of someone other than the owner thereof, and intending and knowing that the offense would injure an owner of those trade secrets,

In violation of Title 18, United States Code, Section 1832 and Title 18, United States Code, Section 2.

Count Two
(Wire Fraud)

From in and around August 1, 2016 through in and around October 12, 2016 in Essex County, in the District of New Jersey and elsewhere, defendant

RALPH MANDIL

did knowingly and intentionally devise and intend to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing and attempting to execute this scheme and artifice, did knowingly and intentionally transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures and sounds, namely, an email dated August 1, 2016 in which he offered to sell proprietary information stolen from his employer, Victim 1.

In violation of Title 18, United States Code, Section 1343, and Title 18, United States Code, Section 2.

ATTACHMENT B

I, Anthony Czajkowski, am a Special Agent with the Federal Bureau of Investigation (“FBI”). I am familiar with the facts set forth herein through my personal participation in the investigation and through oral and/or written reports from other federal agents and law enforcement officers. Where statements of others are related herein, they are related in substance and part. Since 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 and time, I am asserting that it took place on or about the date and time alleged.

The Scheme to Defraud and Sell Stolen Trade Secrets

1. On or about August 1, 2016, defendant Ralph Mandil (“Mandil”) sent an email to a confidential source, who is now working at the direction and under the supervision of law enforcement (“CS-1”), in which Mandil offered to sell CS-1 proprietary trade secrets owned by Mandil’s employer, which will be referred to herein as “Victim 1.” In sending this and other emails in connection with the scheme referenced herein, Mandil used an email address provided by Google, an internet service provider (hereinafter, the “Email Account”). The emails Mandil sent from the Email Account as part of, and in furtherance of, his scheme traveled in interstate commerce.

2. Victim 1 is a privately-held corporation registered in New York that invests, imports and distributes a category of merchandise commonly referred to as “As Seen On TV” products. “As Seen On TV” products include electrical and non-electrical appliances, beauty and personal care, pet care, fitness, auto and outdoor products, which are frequently marketed via television ads, and are commonly sold at large retailers such as Walmart. As a result of its involvement in the “As Seen On TV” market, Victim 1 generates substantial annual revenues.

3. CS-1 works for a company that competes with Victim 1 in the “As Seen On TV” products market. The email Mandil sent to CS-1 on August 1, 2016 offered to provide “inside info on [Victim 1], dropbox access, new product pipeline info [and] factory info” to CS-1, and asked how much CS-1 would be willing to pay for that information.¹

4. After receiving the August 1, 2016 email from Mandil, CS-1, at the direction and under the supervision of law enforcement, exchanged emails and phone calls with Mandil, during which CS-1 purported to be interested in purchasing the Victim 1 trade secrets Mandil was selling, and expressed an interest in meeting with Mandil in person to discuss the offer. In those emails and telephone conversations, Mandil again offered to provide CS-1 with access to Victim 1’s dropbox account, and indicated that the dropbox contained information relating to new products Victim 1 intended to market in the coming months, including sales sheets, product sheets, videos, inventory lists and account lists, among other information. Mandil also advised CS-1 that he wanted to be paid \$197,500 by CS-1 in exchange for the information, which was to be wired to a business account used by Mandil.

¹ A “dropbox” is a personal cloud storage service (sometimes referred to as an online backup service) that is frequently used for file sharing and collaboration. Victim 1’s dropbox is accessible by a limited number of employees (who may access the dropbox from Victim 1’s offices or from remote locations) who are provided with a username and password, which they must enter prior to viewing or editing files stored in the dropbox.

5. At the direction and under the supervision of law enforcement, while under audio and video surveillance, CS-1 met with Mandil on or about September 20, 2016 to discuss the terms of the offer. During that meeting, Mandil advised CS-1 that he was an employee of Victim 1 who was involved in the sale of cookware and other products of Victim 1. Mandil acknowledged that he was the user of the Email Account, and stated that he created the Email Account in order to prevent Victim 1 from discovering his attempt to sell their proprietary information. Mandil also explained that he had access to the dropbox, and estimated that the value of the proprietary information contained in the dropbox could be worth “millions” to a competitor of Victim 1. Mandil further explained that he was offering to sell the information because he was displeased with recent actions taken by Victim 1’s management, which resulted in reduced commissions paid to Mandil.

6. At the direction of law enforcement, during the September 20, 2016 meeting, CS-1 advised Mandil that CS-1 would use the services of a trusted associate to communicate with Mandil and work out the remaining details of the deal going forward. Unbeknownst to Mandil, CS-1 was actually referring to an undercover law enforcement officer (“UC-1”).

7. Following the meeting on September 20, 2016, Mandil continued to send emails to CS-1 regarding the sale of Victim 1’s trade secrets. Additionally, on or about September 23, 2016, Mandil called CS-1 and advised CS-1 that Mandil had some Victim 1 merchandise in his possession, which had yet to be released to the public. Mandil informed CS-1 that Mandil was on his way to New Jersey to personally deliver these items to CS-1’s place of business.

8. During that call, CS-1 attempted to dissuade Mandil from coming to CS-1’s place of business that day. However, Mandil advised CS-1 that Mandil was already in his car and insisted on meeting CS-1 at CS-1’s place of business to deliver the merchandise Mandil had stolen from Victim 1. A short time later, Mandil arrived at CS-1’s New Jersey place of business, met CS-1 in the parking lot, and provided CS-1 with a printout containing details of a proprietary substance used on Victim 1’s cookware, as well as a prototype for another product that Victim 1 planned to bring to market in the near future. Both the details of the proprietary substance and the other product Mandil delivered to CS-1 contained Victim 1’s trade secrets. Upon delivering those items to CS-1, Mandil advised CS-1, in sum and substance, that Mandil believed the information he was providing to be valuable to CS-1.

9. During this meeting on September 23, 2016, as directed by law enforcement, CS-1 again advised Mandil that although CS-1 was interested in the information Mandil was selling, CS-1 wanted to keep a distance from the transaction. CS-1 advised Mandil that UC-1 would contact Mandil to arrange a meeting for the purchase of the remaining proprietary information belonging to Victim 1. Following the meeting on September 23, 2016, CS-1 provided law enforcement with the stolen proprietary information and product of Victim 1 that Mandil had delivered.

10. On September 27, 2016, UC-1, who was outside of New York, called Mandil on the phone number Mandil had provided to CS-1. During that call, Mandil advised UC-1 that he was at Victim 1’s office, which law enforcement knows to be located in New York. During that conversation, Mandil agreed to meet UC-1 at a location in New Jersey to provide UC-1 with an additional sample of the proprietary information Mandil could steal from Victim 1, and further discuss Mandil’s sale of Victim 1’s proprietary information.

11. On or about September 28, 2016, while under audio and video surveillance, Mandil met UC-1 at the pre-arranged location in New Jersey, to discuss the deal in greater detail. During that meeting, Mandil again confirmed that he was the user of the Email Account. Additionally, in an effort to prove that the information he had was valuable, Mandil accessed Victim 1's dropbox via a laptop provided by UC-1. Mandil also provided UC-1 with various samples of merchandise and packaging that Victim 1 would be producing in the near future, which Victim 1 had not yet released to the public. In exchange for this preliminary information, UC-1 provided Mandil with \$10,000 in United States currency.

12. Following the meeting with UC-1, law enforcement met with representatives from Victim 1 to determine the validity of Mandil's offer, and the nature of the threat to Victim 1's trade secrets. Victim 1's representatives confirmed that Mandil was an employee of Victim 1, and that the information stored in the dropbox is proprietary to, and safeguarded by, Victim 1. Victim 1's representatives also explained that a select number of Victim 1's employees are provided with access to the dropbox, which requires a username and password to login, and contains detailed product information regarding all of the items Victim 1 intends to market to the public in the near future.² Victim 1's representatives also confirmed that if a competitor received this information before Victim 1 could release a product to the public, the competitor could use the market data and other proprietary information to obtain a tactical advantage over Victim 1 in the marketplace. In particular, according to Victim 1's representatives, a competitor could steal Victim 1's product designs, undercut its prices and/or push competing products to retailers before Victim 1. Indeed, CS-1 has advised that, in this business, the most important factor in generating revenue is to be the first company to market with new merchandise.

13. Victim 1's representatives estimated that the proprietary information Mandil was offering to sell to CS-1 was worth between \$30,000,000 and \$125,000,000 in revenue to Victim 1 and its competitors.

14. On or about September 28, 2016 and after that date, Mandil conferred with UC-1 via interstate telephone calls, in order to confirm that CS-1 would pay the remainder of the agreed \$197,500 for the purchase of Victim 1's proprietary information. UC-1 and Mandil agreed to meet at a pre-arranged location in New Jersey on October 13, 2016, and Mandil agreed to deliver the login information for Victim 1's dropbox to UC-1 in exchange for the previously agreed sum of money.

15. In the course of, and in furtherance of Mandil's scheme to defraud Victim 1, he made use of interstate wires on numerous occasions by sending emails from the Email Account to CS-1, and making interstate phone calls to CS-1 and UC-1. For instance, on or about August 1, 2016, Mandil sent an interstate email to CS-1 offering to provide Victim 1's proprietary information and access to Victim 1's dropbox. Additionally, on or about September 27, 2016, Mandil, while at Victim 1's offices in New York, engaged in a telephone call with UC-1, who was located in another state, during which Mandil and UC-1 arranged to meet in New Jersey to discuss the terms of Mandil's sale of Victim 1's proprietary information to CS-1.

² At various times, Victim 1's dropbox contains product names, specifications, artwork, advertising, market data and other information, which is safeguarded by Victim 1.