

AO 106 (Rev. 04/10) Application for a Search Warrant

CLERK'S OFFICE U.S. DISTRICT COURT  
AT ABINGDON, VA  
FILED

UNITED STATES DISTRICT COURT

AUG 25 2023

for the  
Western District of Virginia

LAURA A. JUSTIN, CLERK  
BY: *[Signature]*  
DEPUTY CLERK

In the Matter of the Search of  
*(Briefly describe the property to be searched  
or identify the person by name and address)*

Melissa Bandy

Case No. 1:23mj100

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Western District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
21 U.S.C. 331(c), 331(k)	Receipt in interstate commerce of misbranded drugs and offering them for sale. Causing drugs to become misbranded after they have moved in interstate commerce and while held for sale.

The application is based on these facts:

See attached affidavit

- Continued on the attached sheet.
- Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_ ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*[Signature: DA Dobbs]*

Applicant's signature

SA Dustin Dobbs

Printed name and title

*telephonically.*

Sworn to before me and ~~signed in my presence.~~

Date: 8/25/23

*[Signature: Pamela M. Sargent]*

Judge's signature

City and state: Abingdon Virginia

Hon. Pamela M. Sargent, United States Magistrate Judge

Printed name and title

**ATTACHMENT A**

*Description of person to be searched*

1. Melissa Lynn BANDY, DOB XX/XX/1970, SSN XXX-XX-7512, who is a white female, with black hair, brown eyes, approximately 5'05" tall, approximately 120 pounds. A photograph of BANDY is shown below.



**ATTACHMENT B**

*List of items to be seized and searched:*

1. All records relating to violations of *Title 21, United States Code, Section, 331(c) and 331 (k)*, those violations involving Melissa BANDY, including:
  - a. Records and information relating to the shipment or receipt of shipment of Saxenda, Botox, or SelaTox;
  - b. Records and information relating to shipment of Saxenda, Botox, or SelaTox to or from Melissa BANDY or White Orchid Med Spa, LLC;
  - c. Records and information relating to the treatment of customers using Saxenda, Botox, or SelaTox;
  - d. Records and information relating to the advertisement or marketing of Saxenda, Botox, or SelaTox;
  - e. Records and information relating to the sale of Saxenda, Botox, or SelaTox;
  - f. Electronic communications relating to the sale of Saxenda, Botox, or SelaTox;
  - g. Customer records and information, to include payment information, transaction data, and personal information including addresses;
  - h. Records indicating Melissa BANDY performed treatments or sold medical products that would require a licensed medical professional;
  - i. Records indicating a supplier for medical products;
  - j. Records indicating a relationship between Melissa BANDY and a medical provider;
  - k. Communications with customers;
  - l. Communications with vendors;

- m. Bank records;
  - n. Purchase requests;
  - o. Billing invoices;
  - p. Records and information relating to the identity or location of any potential co-conspirators;
  - q. Records and information relating to the identity or location of any other witnesses or victims;
2. Items listed in Paragraph 1 and 1(a) – 1(q) may be stored in a computer (as defined below) or storage medium (as defined below), Therefore, computers and storage medium are to be seized and examined for items listed in Paragraph 1 and 1(a) – 1(q).
- a. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.
  - b. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
3. Computers or storage media used as a means to commit the violations described above, including the receipt in interstate commerce of misbranded drugs and the delivery or proffered delivery of them for pay or otherwise, 21 U.S.C. § 331 (c), and causing a drug to become misbranded after it moved in interstate commerce and while it was held for sale, 21 U.S.C. § 331(k), by dispensing a prescription drug without a valid prescription.

4. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;
  - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
  - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
  - f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
  - g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
  - h. evidence of the times the COMPUTER was used;

- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER or any applications;
  - j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
  - k. records of or information about Internet Protocol addresses used by the COMPUTER;
  - l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
  - m. contextual information necessary to understand the evidence described in this attachment.
5. The compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to a separate warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s), to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of:
- a. any of the Device(s) found at 149 Suffolk Ave, Richlands, Virginia, hereinafter "PREMISES,"
  - b. where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or

instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the Device(s)'s security features in order to search the contents as authorized by a separate warrant.

While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person(s) state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the Device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) is permitted. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, Dustin Dobbs, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the person known as Melissa BANDY, more fully described in Attachment A, for the things described in Attachment B. BANDY is known to operate White Orchid Med Spa, LLC, 149 Suffolk Ave, Richlands, Virginia.

2. I am a Special Agent for the Food and Drug Administration, Office of Criminal Investigation (FDA/OCI), assigned to the Washington Metro Field Office. Prior to my current assignment, I was employed by the Federal Bureau of Investigations (FBI), assigned to the Columbus Resident Agency, Cincinnati Field Office, Ohio, where I worked from February 2018 to December 2022. I have also spent 14 years serving in the United States Air Force from 2009 to present, five years active duty and nine years assigned to Air Force Reserve Command. In my previous position with the FBI, I have experience investigating violations of Title 18 of the United States Code. In my current position with the FDA/OCI, I investigate violations of federal laws including the Federal Food, Drug, and Cosmetic Act (FDCA), Title 21, U.S. Code, Sections 301 – 397, and Title 18 of the United States Code. Based on my training and experience, I am familiar with the rules and regulations governing the drug approval process, methods used to commit fraud against the U.S. Government, and documents and other records that frequently are evidence of such fraud. I am also familiar with how medical products can be introduced into the United States supply chain illegally due to the medical products being foreign unapproved medical products and/or misbranded.



3. The facts and information contained in this affidavit are based upon my training and experience, participation in investigations, personal knowledge, and observations during the course of this investigation, as well as the observations of other agents involved in this investigation. All observations that were not personally made by me were relayed to me by the individuals who made them or are based on my review of records, documents, and other physical evidence obtained during the course of this investigation. This investigation has been worked jointly with the Virginia State Police (“VSP”) and Richlands Police Department (“RPD”).

4. This affidavit contains information necessary to support probable cause. It is not intended to include every fact and matter observed by me or known to the United States.

#### **RELEVANT FEDERAL LAW**

5. The United States Food and Drug Administration (“FDA”) is the federal agency charged with the responsibility of protecting the health and safety of the American public by enforcing the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. §§ 301-399i (the “FDCA”).

6. The FDCA defines a “drug” to include “articles intended for use in the diagnosis, cure, mitigation, treatment, or prevention of disease in man,” “articles . . . intended to affect the structure or any function of the body of man,” and articles intended for use as components of other drugs. 21 U.S.C. § 321(g)(1)(B), (C) and (D).

7. “Prescription drugs” are drugs that, because of their toxicity and other potential for harmful effects, and/or the collateral measures necessary to their use, are not safe for use except under the supervision of a practitioner licensed by law to administer such drugs. 21 U.S.C. § 353(b)(1)(A). A drug is also a prescription drug if the FDA requires it to be administered under the supervision of a practitioner licensed by law to administer such drug as a condition of the FDA’s approval of the drug. 21 U.S.C. § 353(b)(1)(B).

8. A “new drug” is a drug that the composition of which is not generally recognized, among experts qualified by scientific training and experience to evaluate the safety and effectiveness of drugs, as safe and effective for use under the conditions prescribed, recommended, or suggested in the labeling thereof. 21 U.S.C. § 321(p). New drugs may not be introduced into interstate commerce unless FDA has approved an application for that product, either as a new drug application (NDA) for a “pioneer product” or an abbreviated new drug application (ANDA) for a generic version of the pioneer drug. 21 U.S.C. § 355 (a), (j). Sponsors of pioneer drugs must show, among other things, that the drug is safe and effective for its intended uses, as well as submit descriptions of its manufacturing processes and samples of the product and its labeling. An FDA approval of the product is specific to the manufacturer and the specific product considered. Manufacturers of generic products must show, among other things, that their product is bioequivalent to the pioneer.

9. The FDCA imposes many labeling requirements for drugs. A label is defined as the display of written, printed, or graphic matter upon the immediate container of the drug. 21 U.S.C. § 321(k). The definition of labeling is broader and includes all labels as well as other written, printed, or graphic matter upon any article or any of its containers or wrappers or that accompanies such article. 21 U.S.C. § 321(m).

10. The FDCA prohibits the receipt in interstate commerce of misbranded drugs, and the delivery or proffered delivery of them for pay or otherwise. 21 U.S.C. § 331(c).

11. There are myriad ways a drug will be deemed misbranded, including: (i) its labeling is false and misleading in any particular, 21 U.S.C. § 352(a); (ii) its labeling fails to bear required information in the English Language, 21 U.S.C. § 352(c), 21 C.F.R. 201.15(c); (iii) it is a drug sold under the name of another drug or as an imitation of another drug, 21 U.S.C. § 352(i)

and (iv.) its labeling fails to bear adequate directions for the drug's use, as well as any contraindication and warnings. 21 U.S.C. 21 U.S.C. § 352 (f)(1).

12. "Adequate directions for use" is defined in FDA regulations as directions under which the *layman* can use a drug safely and for the purposes for which it is intended. 21 C.F.R. § 201.5. Since prescription drugs by definition cannot be used safely without the supervision of a licensed medical practitioner, it is not possible for there to be adequate directions for *lay* use, and the drugs must qualify for an exemption to this labeling requirement in order to be lawfully distributed in interstate commerce. The exemption for prescription drugs is set forth in 21 C.F.R. § 201.100, which requires all the conditions of the regulation be met, including the drug is: (1) in the possession of a person regularly and lawfully engaged in the manufacture, transportation, storage, or wholesale distribution of drugs; (2) in the possession of a retail, hospital, or clinic pharmacy regularly and lawfully engaged in dispensing prescription drugs; or (3) in the possession of a practitioner licensed by law to administer or prescribe such drugs, *and* the drugs are to be dispensed pursuant to a valid prescription. 21 C.F. R. § 201.100(a). Prescription drugs that are subject to section 505 of the Act (21 U.S.C. 355, or the new drug approval statute) also must bear the labeling authorized by the approved new drug application. 21 U.S.C. § 201.100(c)(2).

13. Prescription drugs will also be deemed misbranded if they are dispensed without a valid prescription from a licensed medical practitioner. 21 U.S.C. § 353(b).

14. Drugs are also deemed misbranded if they are manufactured in a facility that has not been registered with FDA. 21 U.S.C. § 352(o), 360.

15. The FDCA prohibits any person from introducing into interstate commerce any new drug that has not received FDA approval in accordance with the new drug approval statute. 21 U.S.C. § 331(d), 355.

16. One of the products in this investigation is labeled as a cosmetic. Cosmetics are defined in the FDCA as “articles intended to be rubbed, poured, sprinkled, or sprayed on, introduced into, or otherwise applied to the human body . . . for cleansing, beautifying, promoting attractiveness, or altering the appearance.” 21 U.S.C. §321(i). Whether a product is regulated as a drug or a cosmetic (or both) depends on its intended use.

17. The FDCA provides criminal penalties for doing or causing any of the above-mentioned prohibited acts. To establish a misdemeanor, there is no intent or scienter requirement. 21 U.S.C. § 333(a)(1). For a felony, it must be shown that the violation was committed with the intent to defraud and mislead. 21 U.S.C. § 333(a)(2).

#### **IDENTIFICATION OF THE PROPERTY TO BE SEARCHED**

18. This affidavit is submitted in support of a warrant to authorize the search of the person of Melissa BANDY, as more particularly described in Attachment A, which may constitute or contain records, fruits, instrumentalities and other evidence of violations of the above-referenced FDCA statutes.

#### **INTRODUCTION**

18. Based on the information set forth below, your Affiant submits that there is probable cause to believe that between December 2022 and April 2023, Melissa BANDY (hereinafter referred to as BANDY), acquired and distributed and offered for sale Saxenda and SelaTox, received misbranded drugs in interstate commerce and offered them to others for pay or otherwise, 21 U.S.C. § 331(c). Saxenda was misbranded because its labeling was not in the

English language, lacked adequate directions for use, and they were new drugs that did not bear the FDA-approved labeling. The SelaTox was misbranded for labeling that was not FDA-approved as required for new drugs and for lacking adequate directions for use, as well as for being sold under the name of another drug or as an imitation as another drug, and for being manufactured in an unregistered facility. Moreover, Melissa BANDY caused prescription drugs to become misbranded after they moved in interstate commerce and while they were held for sale by dispensing them to customers without a valid prescription in violation of 21 U.S.C. § 331(k), 353(b).

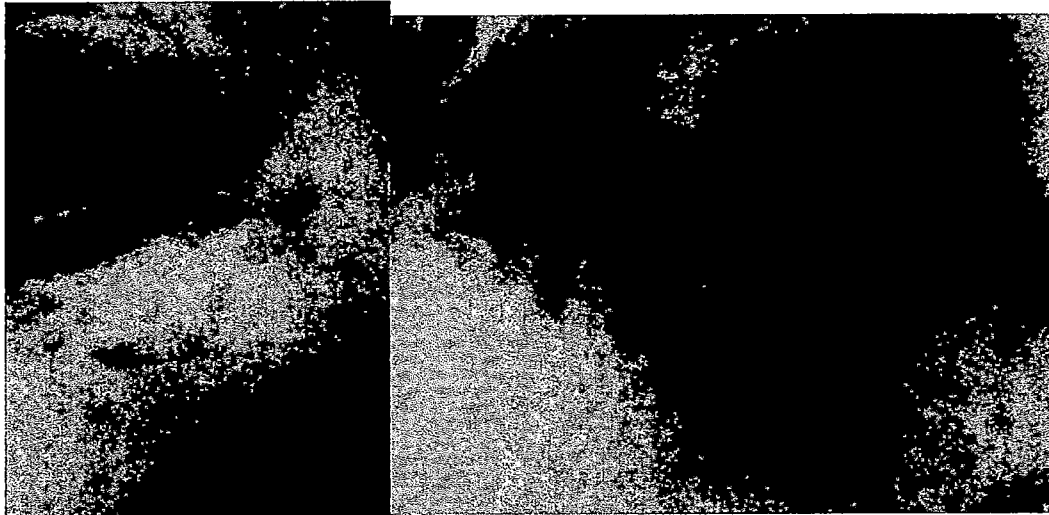
19. The applied-for warrant would authorize the search of this person for the purpose of identifying evidence, fruits and instrumentalities of violations of federal laws, as described more particularly in Attachment B.

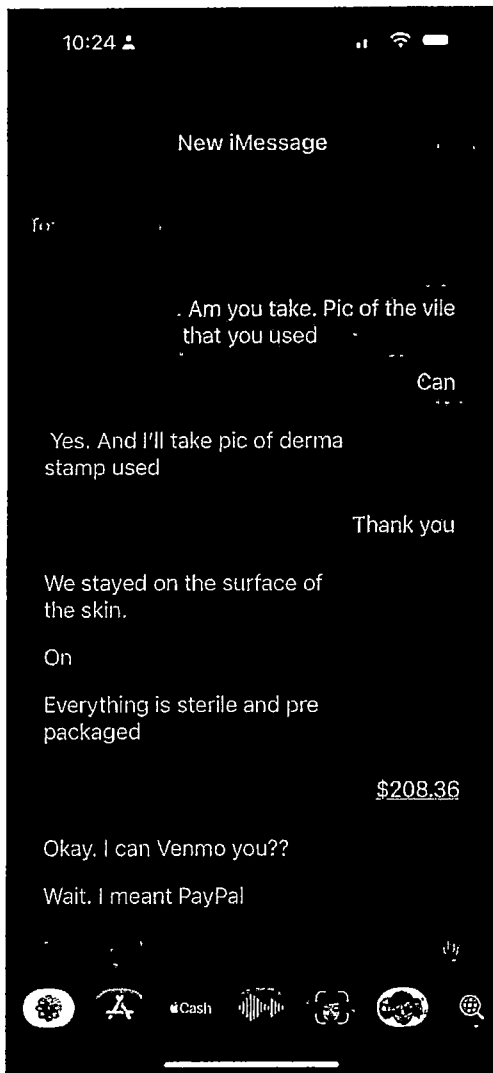
#### *Preliminary Information*

20. Initial information provided to your Affiant by RPD indicated that the owner of White Orchid Med Spa, LLC (“WOMS”), Melissa BANDY, was selling and administering prescription drugs that appeared to be foreign. According to the Virginia Department of Health Professions (DHP) database, BANDY is not a licensed healthcare provider. A complainant told your Affiant that the drugs being sold and administered at WOMS by BANDY were what was believed to be “Botox and Saxenda”. The complainant was aware that the Saxenda being sold by BANDY had foreign writing on it. The complainant had an adverse reaction to what she believed to be Botox injections. The complainant stated that she did not have a medical relationship, such as a doctor-patient relationship, with BANDY or anyone at WOMS. After the complainant had to visit a doctor concerning her adverse reaction, BANDY informed the complainant she had administered SelaTox instead of Botox. The complainant stated that Bandy

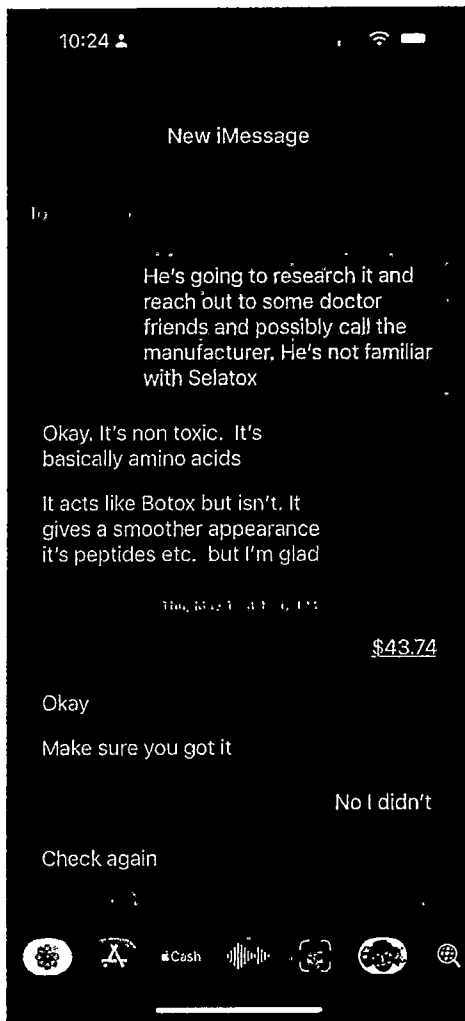
had used injections to administer the SelaTox. Botox generally refers to products derived from botulinum toxin that are indicated to treat wrinkles by paralyzing the facial muscles. There are several FDA-approved botulinum toxin products, and they are prescription drugs. SelaTox is not derived from botulinum toxin, nor is it – as noted below – approved by FDA for any use.

21. Below represents photos taken of the complainant after receiving injections of what she believed to be Botox, the text conversations between BANDY's cellular telephone, telephone number 276-971-1818 (later identified by your Affiant as a mobile phone by Verizon), and the complainant, and a photo sent from BANDY with the actual product used during the injections:





www.courts.ca.gov



22. Your Affiant has been informed, via open-source information, that SelaTox is a product manufactured in South Korean by Sela Cosmetics that is sometimes marketed as an “alternative” to Botox. Its main active ingredient is acetyl hexapeptide. The label on the bottle in the photograph sent to complainant makes the claims that the product is “Anti-wrinkle & Whitening” and is for “Collagen self-generation”. Your Affiant conducted a search of the publicly available database `drugs@fda` (located through `FDA.gov`) for “SelaTox” and “acetyl hexapeptide” and they are not FDA approved drugs. Moreover, Sela Cosmetics is not registered with FDA as a drug manufacturer.



23. According to the complainant, BANDY has also been selling what she believed to be Saxenda for weight-loss. Based on a search of drugs@fda through the fda.gov website, your Affiant is aware that Saxenda™ is a prescription drug containing liraglutide that is manufactured by Novo Nordisk and is FDA approved. According to saxenda.com which was accessed by your Affiant on June 2, 2023, Saxenda is an injectable prescription medicine used for adults with obesity or who are overweight. Saxenda pens must be temperature controlled. There are also several warnings and precautions related to Saxenda such as, risk of thyroid c-cell tumors, acute pancreatitis, acute gallbladder disease, hypoglycemia, heart rate increase, renal impairment, hypersensitivity reactions, and suicidal behavior and ideation. The Saxenda pen that was collected from the complainant as evidence by RPD had what appeared to be only Korean writing on it and therefore could not be an FDA-approved product.

24. According to information provided by the makers of Saxenda, Novo Nordisk, the batch numbers and expiration dates represented on the Saxenda pen collected from the complainant, are tied to Saxenda pens manufactured for the Korean market. Your Affiant is aware that there is not a Novo Nordisk manufacturing location located in the Commonwealth of Virginia. Based upon language used by BANDY in text messages, later described in this document, when discussing purchasing Saxenda, such as “ordering” and “placing another order”; the language used by BANDY in text messages when discussing the receipt of the Saxenda pens, such as “got some more goodies in”, and “your pen is here”; the Saxenda pens sold by BANDY having only Korean writing on them; Saxenda not having a manufacturing facility in the state of Virginia; and your Affiant’s training and experience, your Affiant submits that there is probable cause to believe that BANDY caused misbranded prescription drugs, Saxenda, to enter into

interstate commerce, received them in interstate commerce, offered them for sale, and dispensed them to customers without a valid prescription for pay or otherwise.

*White Orchid Med Spa, LLC*

25. As a result of the initial complaint from RPD, your Affiant conducted a preliminary review of WOMS.

26. FDA's Drug Establishments Current Registration Site indicates that neither BANDY nor her business WOMS located at 149 Suffolk Ave, Richlands, Virginia, is registered as a drug manufacturer.

27. A search of the Virginia Department of Health Professions license lookup reveals that BANDY is not a licensed healthcare provider, medical practitioner, or licensed pharmacy in the state of Virginia and neither BANDY nor WOMS has a wholesale and/or distribution license. No medical license has been discovered during the course of this investigation that would authorize BANDY or WOMS to dispense valid prescription drugs, making any prescription drug that was dispensed by BANDY or WOMS a misbranded drug.

*Victim 1*

28. On June 30, 2023, your Affiant conducted interviews of two additional victims that had purchased what they believed to be Saxenda from BANDY at WOMS.

29. Victim 1 stated she first began a client relationship with BANDY during the summer of 2022 when she became a client at WOMS in Richlands, Virginia. BANDY was the owner and sole operator of WOMS. Victim 1 said BANDY performed several skin treatments on her, including injecting lip fillers, injecting what Victim 1 believed to be Botox, and laser skin treatment.

30. Victim 1 stated she did not have a medical relationship, such as a doctor-patient relationship, with BANDY or anyone else in relation to WOMS. Victim 1 stated that BANDY did not maintain a medical file on her. Victim 1 said BANDY told her she had a relationship with a doctor in Southwest Virginia, but Victim 1 could not remember the name of the person BANDY stated she was affiliated with. Victim 1 believed BANDY had made up this doctor.

31. Victim 1 said she informed BANDY of one of her medical issues without BANDY asking prior to getting a treatment from BANDY. Victim 1 said BANDY never asked her if she was taking any other medication or had any other medical issues. Victim 1 said BANDY never asked her about any potential thyroid issues prior to selling her what she believed to be a Saxenda pen. Victim 1 stated Saxenda carries a risk of thyroid cancer. Victim 1 stated she had a family history and personal history of cancer.

32. Victim 1 stated BANDY sold her what she believed to be two Saxenda pens for approximately \$200 each. Victim 1 said BANDY sent her Saxenda directions that were in English after selling her the pens she believed to be Saxenda. Victim 1 said the pens BANDY sold her had the word Saxenda on them and the rest of the writing was in a foreign language. Victim 1 said after using the pens she had to go to her doctor for blood work due to Victim 1 having blood pressure issues. Victim 1 stated she had to increase her use of metoprolol to treat her hypertension that she believed was caused by the Saxenda medication given to her by BANDY. Victim 1 had previously given the aforementioned Saxenda pen to the complainant who turned it over to Richlands Police Department (RPD). RPD maintained possession of the Saxenda pen as evidence. Your Affiant had an Agent with the ability to read Korean identify the symbols on the pen as Korean writing. No English writing was present on the Saxenda pen other than the word Saxenda.

33. Victim 1 stated she paid BANDY using checks and potentially other methods of payments. Victim 1 stated she spent approximately \$4,000 at WOMS.

34. Victim 1 stated BANDY also gave her what she believed to be Botox injections. Victim 1 said BANDY labeled it as Baby Botox and said, "Baby Botox is what they are doing in Palm Beach." Victim 1 said BANDY's Baby Botox did not work based upon her prior experience with Botox.

35. Victim 1 said she assumed that BANDY was getting her medication from the legitimate supply chain. Victim 1 believed BANDY was legally providing the medical treatments she received.

36. Victim 1 believed BANDY stored the medications, such as Botox and Saxenda, in the back room of WOMS. Victim 1 stated that BANDY went to the back room to get medications when Victim 1 was purchasing them from WOMS.

37. Victim 1 provided your Affiant text messages with BANDY concerning the purchase of Saxenda from BANDY. Below is a verbatim account of text messages that were sent between Victim 1 and BANDY:

December 12, 2022:

BANDY: Hey lady! Your pen is here !

Victim 1: Awesome

Victim 1: Should I run over now. How much do I owe you?

Victim 1: Can I come over now to get it?

Victim 1: I'd you don't mind to send me the directions for the pen so I can start tomorrow. Thanks!

December 13, 2022

BANDY: (Sent a photo of information concerning Saxenda in English with the headings Product Information; How to use; What happens if I miss a dose?; and Do not use Saxenda if.)

December 20, 2022

BANDY: Hey lady. How is the pen doing

Victim 1: Good

Victim 1: I'm not losing weight but my house is full of homemade candy lol

BANDY: Bahhahaha oh my

BANDY: Well I'm okay I'm placing another order if you need anymore

Victim 1: I'll take another one

Victim 1: I just went to 1.2 today

BANDY: Yay

December 29, 2022

BANDY: Hey got some more goodies in. Are you out? Of your pen?

Victim 1: I want a new pen

BANDY: Okay. Got them in this evening. I'll have them at work tomorrow. I have a private party tomorrow but if you'll text me when you get ready to come. I'll run out and meet you and give it to you

January 11, 2023

BANDY: Hey checking in on you. You okay on your pen? I'm placing an order

Victim 1: I had to stop it. My blood pressure and heart rate went up plus I was so constipated.

BANDY: Oh nooooooooooooo

Victim 1: When I got to 2.4 for a few days, it was bad.

BANDY: Oh no. I haven't had anyone do that. How much is left in your pen

Victim 1: I started taking myself down each day and I have very little ready

BANDY: Well I'm god your doing better

*Victim 2*

38. Victim 2 said BANDY was owner and operator of WOMS in Richlands, Virginia.

Victim 2 stated she had bought two or three pens of what she believed to be Saxenda from BANDY at WOMS. Victim 2 said the two pens had foreign writing on them. Victim 2 said medicines often have poor effects on her. Victim 2 stated she did not see any results from the weight loss drug sold to her by BANDY.

39. Victim 2 said BANDY never mentioned having a supplier for her prescription medications. Victim 2 believed BANDY to be licensed and authorized to sell Saxenda. Victim 2 said because of this belief she never questioned the supply chain for the medication that she was receiving from BANDY. At the time of the interview, Victim 2 believed BANDY may have bought the medication from an online retailer.

40. Victim 2 said BANDY had approximately 13 or 14 clients that were taking Saxenda at the time of her first purchase. Victim 2 said BANDY informed her of this when marketing Saxenda to her.

41. Victim 2 stated she also had "injections" in the bags of her eyes with no result. Victim 2 did not remember what BANDY injected into her face below her eyes. Victim 2 said this treatment was not effective. Victim 2 said she also had laser skin tightening done by BANDY at WOMS.

42. Victim 2 said she spent approximately \$5,000 at WOMS. Victim 2 said she either used cash or credit card to purchase what she believed to be Saxenda.

43. Victim 2 said BANDY asked Victim 2 if she had any allergic reactions to medicine prior to Victim 2 purchasing what she believed to be Saxenda from WOMS. Victim 2 did not have a medical relationship, such as a doctor-patient relationship, with BANDY or anyone associated with White Orchid Med Spa.

44. Victim 2 voluntarily provided your Affiant with what she believed to be a Saxenda pen and the box it came in that she had purchased from BANDY at WOMS. Victim 2 said this was the second or third Saxenda pen she had purchased from BANDY. Victim 2 said she only used some of the pen given to your Affiant before she quit taking it because she realized it was not working. The Saxenda pen and the box it came in that was collected from Victim 2 as evidence by your Affiant had what appeared to be only Korean writing on it and therefore could not be an FDA-approved product.

#### *Internet Presence*

45. On June 1, 2023, Your Affiant reviewed the website [whiteorchidmedspa.com](http://whiteorchidmedspa.com). The website showed that BANDY has been practicing as a licensed aesthetician and cosmetologist for over 30 years. The website advertised that WOMS conducts microneedling, microblading, nano mesotherapy or meso Botox, and baby Botox and hydra derma stamping. Under the contact tab, the website states “(f)or more information on services, to book an appointment, and/or contact me directly, please call/text 276-971-1818”. Under the other services tab of the website, a picture (depicted below), depicted below, shows BANDY sitting behind a patient with a table with what appear to be needles on it.



46. On June 1, 2023, SA Dobbs reviewed BANDY's Facebook page. BANDY's public Facebook page shows that BANDY is the owner of WOMS in Richlands, VA. BANDY's Facebook page also showed microneedling treatment before and after pictures attributed to work being performed at WOMS.

47. On June 28, 2023, your Affiant attempted to review the website whiteorchidmedspa.com. The website appeared to be taken down.

48. On July 12, 2023, your Affiant and SA Peery of the VSP, performed surveillance of the PREMISES identified as 149 Suffolk Ave, Richlands, Virginia. A BMW X1 registered to BANDY was parked in the back of the PREMISES and a dark-haired female that appeared to be BANDY was working inside the business.

**TECHNICAL TERMS**



49. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

**COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

50. As described above and in Attachment B, this application seeks permission to search for records that might be found on the person of BANDY, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

51. Probable cause. I submit that if a computer or storage medium is found on BANDY, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”
- e. Based on actual inspection of documents and evidence related to this investigation, I am aware that computer equipment was used to generate, store, and possibly print documents used in connection with violations of the FDCA. There is reason to believe that there is a computer currently located on the person of BANDY.

52. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes

described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the possession of BANDY because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information,

communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpatng or exculpatng the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a

digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular

thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

53. Necessity of seizing or copying entire computers or storage media. In most cases, a thorough search of a person for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the area of the person, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time in the area of the person could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data during the search. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

54. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

55. White Orchid Med Spa LLC (“the Company”) is a functioning company that conducts legitimate business. The seizure of the Company’s computers may limit the Company’s ability to conduct its legitimate business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and

what computers or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If employees of the Company so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of the Company's legitimate business. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

*Biometric Access to Device(s)*

56. The warrant I am applying for would permit law enforcement to obtain from the person of Melissa BANDY (but not any other individuals present at the PREMISES at the time of execution of the additional federal search warrant for the PREMISES) the compelled display of any physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices requiring such biometric access subject to search and seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s) physical biometric characteristics will unlock the Device(s). I seek this authority based on the following:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of



these biometric features, and the user of such devices can select which features they would like to utilize.

- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.
- c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Android's "Trusted Face") have different names but operate similarly to Face ID.
- d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows

Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

- e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- f. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.
- g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers,

that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours and the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

- h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) if reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of BANDY and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.
- i. The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). Nor does the

proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

### CONCLUSION

57. Based on the above described facts and circumstances and my training, knowledge, and experience, your Affiant submits there is probable cause to believe that between December 2022 and April 2023, in the Western District of Virginia, Melissa BANDY committed the offense of receiving misbranded drugs in interstate commerce and offering them for sale (labeling not in English language, labeling not bearing adequate directions for use because it was not the labeling approved by FDA, drugs from unregistered facility, drug offered under name of another drug or as an imitation of another drug) as well as causing drugs to become misbranded after they have moved in interstate commerce and while they are held for sale by dispensing them without a valid prescription when BANDY distributed the unapproved and misbranded prescription drug Saxenda and administered the unapproved and misbranded drug SelaTox to

customers at White Orchid Med Spa, LLC. I submit that this affidavit supports probable cause for a warrant to search the person, Melissa BANDY, described in Attachment A and seize the items described in Attachment B.

Signed and sworn to this 7 day of August, 2023.

D.A. Dobbs  
Dustin Dobbs  
Special Agent

telephonically  
Subscribed and sworn to before me on Aug 25, 2023:

Pamela Meade Jax  
UNITED STATES MAGISTRATE JUDGE