AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Colorado

United States of America v. FILIP LUCIAN SIMION, LEONARDO CRISTEA, YMRAN DJAVATKHANOV and ANDY NESTOR *Defendants*	))))))	Case No. 16-mj-01032-NYW

AMENDED CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief: On or about the date(s) of 1/19/13 through 3/16/16, in the State and District of Colorado, and elsewhere, the defendants violated:

Code Section	*Offense Description*
21 U.S.C. § 846	Conspiracy to Distribute Controlled Substances
21 U.S.C. § 963	Conspiracy to Import Controlled Substances into United States

This criminal complaint is based on these facts:

See Affidavit attached hereto and herein incorporated by reference.

X Continued on attached sheet.

s/Ryder K. Wells
Complainant's signature

Special Agent Ryder K. Wells, HSI
Printed name and title

Sworn to before me and: ☐ signed in my presence.
☒ submitted, attested to, and acknowledged by reliable electronic means.

Date: ***16 Mar 2016***

Nina Y. Wang
Judge's signature

City and state: Denver, Colorado

United States Magistrate Judge
Printed name and title

AMENDED AFFIDAVIT IN SUPPORT OF ARREST WARRANTS

I, Ryder K. Wells, being duly sworn, do hereby depose and state:

1. Your affiant submits this amended affidavit in support of an amended complaint seeking arrest warrants for FILIP LUCIAN SIMION, LEONARDO CRISTEA, YMRAN DJAVATKHANOV, and ANDY NESTOR for violations of Title 21, United States Code, Sections 846 and 963, conspiracy to distribute and import controlled substances.

2. I am a Special Agent of U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), assigned to the Office of the Special Agent in Charge, Denver, Colorado. I have been in this position since May 2005. I am assigned to the Cyber Crime Investigations Group. I successfully completed the Criminal Investigator Training Program and Special Agent Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia. Before joining HSI Denver, I received a Bachelor of Environmental Design degree, Architecture Emphasis, from the University of Colorado at Boulder. As part of my duties with HSI, I have received training and instruction in the field of investigation of criminal offenses relating to money laundering and narcotics smuggling and distribution. I have personally participated in investigations, seizures, and prosecutions relating to these violations, including complex cybercrimes employing schemes of both fiat and virtual currencies. I have received training in the manner and means by which individuals use computers and the Internet to commit crimes.

3. I am familiar with the methods employed by drug smuggling and money laundering organizations to conduct their business, including, but not limited to: their methods of importing and distributing narcotics; the transportation routes and means of

coordination which supply country organizations use to smuggle narcotics across the U.S. border, including the use of international and U.S. mail systems; the methods of laundering the profits derived from the sales of controlled substances; the use of telephonic, electronic, and other telecommunications methods to conduct drug transactions and launder drug proceeds; the use of the Internet via anonymization tools, namely the "dark web" or "darknet" to distribute and purchase drugs; and the use of encrypted email and communication apps such as Whisper, WhatsApp, Wickr, Snapchat, Telegram, RedPhone and Signal from Whisper systems.

4. The facts in this affidavit come from my personal knowledge, my training and experience, and information obtained from other law enforcement officers involved in this investigation, including foreign investigators and prosecutors. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

BACKGROUND OF THE INVESTIGATION

5. In July 2013, the U.S. Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) and the U.S. Postal Inspection Service (USPIS) in Denver, Colorado began investigating money laundering and drug trafficking activities involving online black markets located on the "dark web" of the Internet.[1] These online markets, such as "Silk Road", "Agora", "Black Market Reloaded", and "Sheep Marketplace", offered controlled substances and other illegal goods for sale anonymously utilizing the digital currency bitcoin.

[1] The "dark web" is a portion of the "Deep Web" of the Internet, where individuals must use an anonymizing software or application called a "darknet;" the most prolific of these is the "Tor" network, or "The Onion Router," utilized to access certain websites such as online marketplaces.

6. As part of the investigation, Denver HSI agents and postal inspectors arrested and/or interviewed several individuals in the District of Colorado who ordered distribution quantities of MDMA from the online vendor "ItalianMafiaBrussels," aka "IMB." IMB first appeared on the Silk Road darknet market on January 19, 2013. IMB later transitioned its operation to Silk Road 2.0 after law enforcement's seizure of the original Silk Road. Eventually, the IMB organization directed its customers off of the marketplaces, giving instructions for direct communication and online orders via encrypted email. As described below, your affiant believes that FILIP LUCIAN SIMION, LEONARDO CRISTEA, YMRAN DJAVATKHANOV, ANDY NESTOR, and others, are members of a conspiracy, a drug trafficking organization, operating online as the MDMA vendor "ItalianMafiaBrussels," aka "IMB."

PROBABLE CAUSE

7. On June 14, 2013, U.S. Customs and Border Protection (CBP), Port of Cincinnati, intercepted a parcel from Belgium addressed to an individual (a cooperating defendant referred to below as CD-1) in Boulder, Colorado. The parcel contained 60.9 grams of MDMA. Boulder County Drug Task Force conducted a controlled delivery of the parcel, and the recipient (CD-1) agreed to cooperate with law enforcement regarding the source of the parcel.

8. On July 19, 2013, agents interviewed this Boulder County Drug Task Force cooperating defendant (CD-1) regarding his online purchases of MDMA from a vendor operating on the darknet marketplace Silk Road, ItalianMafiaBrussels. CD-1 explained how he accessed the darknet using the Tor browser and how he obtained bitcoin from a local bitcoin exchanger in Boulder to purchase the drugs.

9. Agents reviewed data recovered from the Silk Road server[2] and confirmed CD-1's purchases of MDMA from IMB. According to the data, on February 16, 2013, CD-1 purchased $654.07 worth of MDMA from IMB. Order details showed the product description as "*28g Pure MDMA 80% Labtest Best Quality/Price.*" In addition, on March 3, 2013, CD-1 posted the following comment regarding the order:

> *Relatively quick shipping and decent stealth. All powder, no crystals unfortunately. Product looks good though, certainly not the best on the road, but worth the money. Weighed in .7 under. Overall 4/5 experience. Would buy from again.*

10. In September of 2014, the Belgian Federal Judicial Police (Federale Gerechtelijke Politie, or "FGP"), East Flanders Drug Unit in Dendermonde, Belgium advised your affiant about the seizure of numerous drug parcels between February and September of 2014. The parcels were returned to Belgium as undeliverable to U.S. addresses. The owner of a company in Belgium selling model train parts online, Modeltrein Paradise, called police after receiving a parcel he did not recognize containing drugs. The FGP reported that 19 parcels seized were mailed from the Ghent area of Belgium and contained 6 to 259 grams of MDMA each, packaged in mylar-type bags with false invoices from various legitimate online businesses, including Modeltrein Paradise. A comparison of the invoices and packaging revealed significant similarities, leading the FGP and your affiant to believe that the parcels were mailed by the same individual or organization.

11. FGP investigators also received Silk Road server data, reviewed communications of MDMA vendor ItalianMafiaBrussels, and determined the following:

---

[2] On October 2, 2013, federal agents seized the Silk Road server in conjunction with an investigation led by the Southern District of New York. On November 6, 2014, as part of Operation Onymous, agents seized the Silk Road 2.0 server. Data from both servers were made available to law enforcement, including agents investigating this case.

IMB is fluent in Dutch[3] and English and uses Flemish expressions; IMB talked about Romania; IMB talked about police profiling and used the acronym for the Belgian Federal Judicial Police, "FGP;" in 2013, IMB claimed to be living in the Flemish part of Belgium, near Brussels.

12. In March of 2014, agents identified an individual (referred to below as CD-2) in the Denver, Colorado, area involved in the distribution of MDMA purchased from darknet marketplaces. In May of 2014, the individual was charged by a federal grand jury in the District of Colorado with conspiracy to distribute MDMA. This defendant (CD-2) pled guilty and agreed to cooperate with law enforcement.

13. In July, August, and September of 2014, agents interviewed CD-2. CD-2 stated that he had purchased MDMA from the vendor ItalianMafiaBrussels, among others, who he believed, based on communications with IMB, was located in Belgium and had a "crew" in Belgium. CD-2 stated that he believed IMB bought in bulk from a manufacturer. CD-2 stated that the packages received were brown to light tan in color and had printed labels from a "soap company," with an invoice indicating that the parcel contained bath salts and including directions on how to use the "bath salts" in a bathtub. CD-2 stated that no tracking was employed and that blue stamps were typically used. CD-2 stated that he had received two packages of MDMA powder/crystals from IMB in the summer of 2013 (approximately 50 grams and 150 grams, respectively) and two packages in the fall of 2013 (200 grams each). CD-2 stated that he ordered an additional 200 grams at the end of fall 2013, which never arrived, but IMB re-shipped 100 grams that he subsequently received in December of 2013. CD-2 stated that he initially received the packages at an apartment in Denver, Colorado, and he recalled

[3] Dutch is the predominant language used in Belgium.

that the fictitious company name marked on the packages (return address entity) was "Soap Story."

14. Agents reviewed data recovered from the Silk Road server and confirmed CD-2's purchases of MDMA from IMB on May 19, 2013, July 11, 2013, August 6, 2013, September 10, 2013, and October 1, 2013. His order details showed a product description of "*100g Pure MDMA 80% Labtest Best Quality/Price*" for each, and the prices paid for the orders were $1,887.32, $1,794.37, $3,544.94, $3,484.44, and $3,481.24, which indicated that the last three orders were each doubled from the first two, for an approximate total of 800 grams of MDMA. A notation from server information relating to the final order indicated that the order was, in fact, not originally received.

15. In March of 2014, agents identified another individual (referred to below as CD-3) in the Denver, Colorado, area involved in the distribution of MDMA purchased from darknet marketplaces. Agents conducted online searches of the username utilized by this individual and determined that he had purchased MDMA from the vendor "ItalianMafiaBrussels" on the Silk Road. A posting on February 27, 2014, indicated that the individual had not received his latest order from IMB. Postings also indicated that the vendor utilized the e-mail address "italianmafiabrussels@safe-mail.net." In July of 2014, the individual was charged by a federal grand jury in the District of Colorado with conspiracy to distribute MDMA. This defendant (CD-3) pled guilty and agreed to cooperate with law enforcement. During a search of CD-3's Silk Road account after his arrest, agents discovered communications with IMB regarding MDMA orders and IMB's ratings.

16. On July 25, 2014, agents interviewed CD-3. CD-3 stated that he had purchased MDMA from the vendor ItalianMafiaBrussels on Silk Road and Silk Road 2.0, among others. CD-3 recalled an IMB posting on the Silk Road forums that they had lost $250,000 when the first Silk Road website went down. CD-3 stated that he had purchased numerous packages containing MDMA from IMB, totaling approximately one kilogram. CD-3 stated that the last time he purchased from IMB was approximately 7 to 8 months prior, around December of 2013. CD-3 stated that the packages would be sent under the name of a bath salts company and would contain an invoice. CD-3 stated that the packages arrived from Belgium and were wrapped in a soft mail envelope and bubble wrap, and the MDMA was sealed within a mylar-type bag, placed inside the other packaging.

17. Agents reviewed data recovered from the Silk Road server and confirmed that CD-3 purchased 250 grams of MDMA from IMB on August 6, 2013; the corresponding order details showed a product description of "*250g Pure MDMA 80% Labtest Best Quality/Price,*" and the price paid for the order was $4,336.11. In addition, the data showed that on October 1, 2013, CD-3 made a purchase of 700 grams of MDMA from IMB; the corresponding order details showed a product description of "*700g mdma custom*," and the price paid for the order was $11,588.46. A notation from the server information corroborated CD-3's claim that one of the packages he ordered did not arrive. Agents also reviewed data recovered from the Silk Road 2.0 server. The data confirmed CD-3's MDMA orders to IMB on December 21, 2013, and January 16, 2014, with the January order being a re-ship of a previous order not received.

18. On or about October 14, 2014, CBP officers at JFK airport intercepted a mail parcel from Belgium, addressed to an individual in Ann Arbor, Michigan, containing approximately 256 grams of MDMA. On October 22, 2014, HSI agents and local and state police, with the assistance of the Postal Inspection Service, conducted a controlled delivery of the parcel in Ann Arbor, Michigan. On October 23, 2014, investigators arrested an individual (referred to below as CD-4), who admitted to ordering distribution quantities of MDMA online from darknet marketplace drug vendors using the digital currency bitcoin.

19. On January 16, 2015, and January 7, 2016, agents interviewed CD-4. CD-4 confirmed that he had ordered MDMA from a Silk Road vendor using the name "ItalianMafiaBrussels." CD-4 stated he also purchased MDMA from IMB on Silk Road 2.0 after the first Silk Road server was seized by law enforcement and then transitioned to direct transactions, using encrypted email with IMB outside of the markets. CD-4 stated that IMB changed his bitcoin address once a month. CD-4 confirmed his own username on Silk Road and that he had ordered crystal rock MDMA. CD-4 stated that he conducted several transactions with IMB and that the last purchase was for 500 grams, which was divided into two shipments of approximately 250 grams each. CD-4 described the packages received from IMB as white or yellow-manila padded envelopes addressed from a Belgian soap company that sold “bath salts.” CD-4 stated that the interior of the parcel carried an invoice that contained directions on how to use the "bath salts" and that the MDMA was concealed in black, mylar-type bags. CD-4 recalled a conversation over email in which IMB indicated that he/they had lost 400,000 Dollars or

Euros in a hack of IMB's accounts. CD-4 also stated that he had the MDMA parcels ordered from IMB mailed to various drop locations in Ann Arbor, Michigan.

20. From on or about August 2015 through March of 2016, a Denver HSI agent acting in an undercover capacity (hereinafter referred to as "HSI UC") conducted online communications with IMB using undercover email accounts. The HSI UC communicated, at IMB's request, by PGP encrypted messaging on a Tor-based email website called Sigaint. Initially, IMB used the email address "italianmafiabrussels@safe-mail.net" and then transitioned to the use of the email address "xxxxxxxxxxxxxxx@sigaint.org." The HSI UC and IMB exchanged multiple emails discussing PGP key encryption and the purchase and delivery of MDMA to Colorado. On August 29, 2015, the HSI UC account received an encrypted email message from IMB at italianmafiabrussels@safe-mail.net. The message gave instructions for contacting IMB going forward and provided several different email addresses.

21. On September 2, 2015, the HSI UC received an email from IMB in an encrypted format using the email address "xxxxxxxxxxxxxxx@sigaint.org." The message described IMB's transition from a MDMA vendor affiliated with online darknet marketplaces such as Silk Road and Silk Road 2.0, to direct, peer to peer MDMA sales:

> *Hello mate,*
> *First of all i want to show you a bulk message that i used to send to all my old customers coming back here for private sales, i will show it to you, and then i will reply to the rest of your message:*
>
> *I am happy to tell that my new shipping methods are working smoothly now, i ship from about four different countries to maintain a low profile and succesfully prevent profiling of my stealth.*
>
> *If i can manage to get enough bulk buyers to sell about 1-2kg of MDMA per week "wallet-to-wallet" then i will never sell on a public market again.*

This way i avoid attention of Police and i avoid seizures and other problems.. I wonder if i were to say the following things to you (it guarantees you more safety and consistency) if you would keep ordering from me exclusively, wallet-to-wallet.. Please read ahead..

You know, the thing is, it's difficult to keep vending publicly without once your packs being profiled, and a wave of seizures following.. I have been in this game for long and know the patterns all too well... So this is my plan now.. I am just looking for some trustable long term clients that will stick with me, so that i sell my product well week after week, and we can continue running this operation safely for much time, without worrying about cops seizing our packs too much..

My fixed price for MDMA is 11 USD per gram wallet-to-wallet, and that's maybe 1 USDmore than some other vendors, but keep in mind what i've just said.. None of these big public vendors will be able to keep it flawless, and none offer the 100% reship rate I always did.. I always delivered, wether that made me broke or not (it did in the last couple of months)

The minimum ammount for ordering wallet-to-wallet is 250g, and that will come in one pack.

The XTC pills I currently sell are 180mg and come at a flat rate of 2.8USD per pill, Current batch are Orange Supermans.

Look i have kept my mouth shut because they asked me, but i can tell you even more. Most of these other big vendors from europe, have been contacting me through the whole summer, complaining about their massive ammount of seizures. They were very good at hiding the real damage though, they would answer PM's quickly and ask people explicitely to not post about it on the forums. A LOT OF MDMA GOT SEIZED, not only mine. Few other vendors had way more weight seized than i did.

But me, i was the one that was trying to be the most honest one by instantly telling everyone on the forums that i had large seizures happening, for god sake's everyone's safety. I have saved a lot of guys from jailtime by warning them, and they are now thankful to me. All that While the other vendors were doing their best to keep it 'a little secret' as much as possible. My honesty kind of has bitten me in the ass, it made me look like i have had the most seizures.. But from the ammount of KG that the other vendors told me they have lost, it really shocked me.

This is some insider info i am sharing with you, please do not start gossiping around that i have told you this, i don't want to look like i am back-talking people, i just wanted to give you the full explanation why *being a big public vendor now is just nuts, because of LE profiling them.. And from a customer's point of view, it's dangerous to order from most public big vendors, most of them don't give a fuck if you are behind bars or not, all they care about is getting you to SHUT UP SO THEY CAN KEEP LOOKINGFLAWLESS and keep making those big sales.. while some people go to jail, by overconfidently picking up their package (why would they not, everything seems "FLAWLESS" in the their vendor's feedback). They keep looking flawless by several ways:*

1) Asking you not to write anything on the forums and keep quiet

2) Teling you to first leave a perfect feedback before they send your reship

You can now see.. Besides that, from now on, with the Europol operation (Operation Onymous), perhaps it's smarter to be very careful with any vendor. I have known quite some vendors over the darknet from Europe, and let me tell you, most of them are basically kids.

I have no doubt most of these vendors would instantly fully co-operate with the cops at the first second of getting busted. Some of them are addicted to drugs (you can sometimes see it on their way of typing), run their operation very sloppy. Often they make critical mistakes, like going partying with flash cars while leaving their encrypted computer OPEN at home.. Which has their marketplace login details PGP keys; and shipping addresses on it.. None of that you get to see..

Then scenario's happen like police kicking the door open and taking away a live open Darknet work computer.. All because these kids from the Netherlands/Belgium/Germany take darknet vending as a little safe side-job that they can easily make loads of money with; and not care too much about getting busted since first-time offences range from 6 months to 24 months imprisonment anyways (and they could be out in less than half the sentence time on parole).

But these kids don't realize that people in other countries they are doing business with could be risking fucking 5-20 years for receiving these packs, and THAT'S exactly where my anger gets directed to, how these fools could only are about their own safe asses. They are always very good at trying to appear "loyal" and "caring" on their fakeassdarknet persona, ofcourse just to keep those sales going, as long as they are not busted the smile is on their face..

The Europol notice definitely says there were arrests in countries like "Germany, Netherlands" (two of the 16 countries listed) just one more thing to be aware of.. I can tell you dozens of more stories.. Because of the generally low sentences in western-europe, most drug dealers here *are not serious for a second. They are good at masking it all though and appear all "Strong OPSEC"; remember SuperTrips with this "We are never going to get caught" claims on his profile page, and everyone seeing him as the "Untouchable King" ? Well he was basically probably the dumbest vendor ever in the area.. He got caught by making the most stupid basic mistake a vendor could make, not wearing gloves when shipping his stuff. Guy got caught, handed over his whole account to the cops, and took down 12 real-life drug dealers among with him, from the Netherlands.*

I hope this long explanation has given you a bigger idea about what's sometimes going on here in Europe, i could tell some more things that would scare you off even more from ordering from other vendors, but i think you get the picture by now.. You don't want to know how many of these other vendors are having real-life links, andget close to each other. Just one of them has to be nabbed and potentially all their accounts could become LE honeypots.

Please keep this insider info for yourself, i don't want this to leak out.. This is really private info, i kind of hate gossiping, but considering this has to do with saving persons from jail, and i can somewhat trust you, because you have been a long term client of me, i feel like it's my duty to tell you this.

Me personally i have always stayed far away from them, i have never ever (and never will) meet with someone in real life that i have met on the darknet, or met in regards to anything darknet related. Never ever, and this simple rule is one of the multiple things that have kept my operation safe, besides the other strict OpSec methods we use here to keep everyone safe.

I hope that with this message i could have set you in a more conscious place to decide whom you want to continue your business with !

=================

As to reply, i've got some 180mg red speakers currrently, they are bomb pills? Or i got M for 11 USD per gram. You want something?

Here's everything you need to know if you wish to place an order:

*!!!!! Please carefully read further, because the instructions have changed a bit to how it was in the past**

Here are my instructions for you to place a new order wallet-to-wallet; Read everything CAREFULLY ahead..

The price for the MDMA is 11 USD per gram (flat rate for any quantity); Minimum order250g

The price for the 180mg XTC pills ("RED SPEAKERS") is 2.8USD per pill (flat rate for any quantity): mininum order 1000 pills;

Every new order will have a new individual BTC deposit address, this address stays valid for a while after i've sent it to you, i just hope you send the bitcoins within 14 days of receiving this BTC address

! WARNING!, it only stays valid for a while if the payment is not yet done. Once the payment is made, the address can become invalid at any second, Because i delete addresses once the payment is made over. Theoretically i don't delete any address until you have made a payment; But i just prefer to set a 14-day deadline to avoid any mis-understandings.

! WARNING! It is your responsability to not make any mistakes here. Any additional BTC sent after an order was completed, are going to be LOST, and that is YOUR LOSS. So please be extra careful, EVERY TIME; Never make the mistake of using one BTC address twice, every new order placed, has a different bitcoin address!

*! NOTE: Only send me out the the payment info once you see that *ALL BTC* have actually landed in my wallet. You must manually check my bitcoin address on the Blockchain, to see if the bitcoins have actually landed.*

This way we avoid confusion if the coins are still on their way, and my bitcoin wallet isstill empty at the time you send your message.

*So basically: *One transaction* per BTC address, *One order* per BTC address. Please never send multiple transactions, or make multiple orders, to the same deposit address.*

The Deposit address for this transaction is:
!!!
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX59N2
!!!

Send me the right ammount of bitcoins according to the BITSTAMP rate, then provide me ONE message with the following accurate info;

-Order size (price)
- RATE USED x BTC SENT = MONEY SENT
- BTC address sent FROM, and sent TO
- Shipping address

> *After i verify this info i ship out within 24-48 hours.*
> *Note that from now, the reship policy for the packs is set back at fifty percent, because of some recent misabuse of the policy.*
> *Regards*

22. Using the procedure IMB outlined, the HSI UC purchased 1,000 pink in color, speaker-stamped ecstasy pills by sending IMB 11.5 BTC to a designated bitcoin address. At the time of purchase, 11.5 BTC was worth approximately $2,804.39. On October 6, 2015, agents received a parcel postmarked from France at an HSI undercover address in Colorado. The outside of the parcel was white in color, with a Republique Francaise 8,50 EUR postage and a postmark dated September 26, 2015. The reverse side of the parcel had the address "36 Rue Damremont, 75018 Paris, France." The interior of the parcel had a black moisture barrier bag (MBB) with the label "CRYSTALITAS SPIRITUAL COMMUNITY ROUCH ORANGE CALCITE" affixed to the MBB bag and an invoice. The invoice was dated "09222015" and was labeled as from "Crystalitas Spiritual Community" and that it contained "ROUGH ORANGE CALCITE 250Grams." Inside the MBB bag was a vacuum sealed clear plastic bag double wrapped around pink tablets. The parcel contained 997 pink tablets, plus pieces, marked with a speaker logo. Agents conducted a field test of the tablets which tested presumptively positive for the presence of MDMA. The gross weight of the MDMA was 272.7 grams.

23. In December of 2013, the FGP West Flanders Drug Unit in Bruges, Belgium conducted a drug investigation into the activities of FILIP LUCIAN SIMION. On December 5, 2013, the FGP executed a court authorized search warrant on SIMION's residence located in Ghent, Belgium. During the search, police seized €17,759 in cash,

financial documents, electronic equipment, an Apple iMac computer, several identical cheap mobile phones, pre-paid SIM cards (still in packaging), and a gray Mini Cooper registered to SIMION. The computer had full-disk encryption and could not be examined by Belgian police; however, inside the vehicle police found and seized a receipt, dated March 12, 2013, reflecting the purchase of hundreds of pieces of packing and shipping materials, including boxes and envelopes designed to protect the contents against shock damage. The envelopes purchased were described as brown in color with bubble/blister padding, similar to the envelopes used by IMB.

24. In addition, the FGP identified a garage located at Naarstigheidstraat 80, 9300 Aalst, Belgium, which was rented by SIMION under the name Jonathan Levieux. During the investigation, investigators observed SIMION's Mini Cooper at the garage, and neighbors reported seeing the Mini Cooper at the garage on a daily basis, usually late at night. On December 9, 2013, the FGP West Flanders Drug Unit executed a court authorized search warrant on the garage. Inside the garage, investigators discovered packaging materials, including envelopes and mylar-type/foil bags; hundreds of rubber gloves; invoices, including invoices for "Soap Story," a company selling bath salts; two Belgian Post (Bpost) international shipping forms with tracking numbers, and 21 printed mailing labels (17 bearing U.S. addresses). One of the mailing labels found listed CD-3's name and address in Thornton, Colorado, and two other mailing labels corresponded to addresses in Ann Arbor, Michigan used by CD-4 for MDMA orders from IMB. There were also mailing labels for "Soap Shop" with different addresses in Belgium. The "Soap Story" and "Soap Shop" invoices and labels appeared to be the

same as those used by IMB to disguise MDMA shipments. Investigators did not find any controlled substances.

25. The FGP interviewed the owner of the garage who stated that a person using the name Jonathan Levieux rented the garage and used a document, "Proof of declaration of the loss, theft, or destruction of an identity card,"[4] as identification for the rental contract. The owner provided police a copy of the Levieux document; the document contained a photograph of FILIP LUCIAN SIMION. The FGP subsequently determined that on August 14, 2012, FILIP LUCIAN SIMION filed a police report and obtained a certificate of loss in Bruges. Comparison of the SIMION and Levieux certificates confirmed that SIMION used his original certificate to create the false document in the name of Jonathan Levieux.

26. Belgian police conducted searches of business registration information and found FILIP LUCIAN SIMION listed as one of the business managers (legal persons) for the company "VOF ROXR Group" (ROXR). The following information was also available relating to ROXR: "Date of establishment: 01/07/2013," and "Company capital: 400,000 EUR represented by 150 shares." Each party has 50 shares. Belgian investigators indicated that the volume of business for ROXR did not support the stated capital, and suspected it as a front company.

27. In the spring of 2015, the FGP East Flanders Drug Unit in Dendermonde, with the assistance of other European police authorities, including the Romanian Federal Police, began conducting surveillance of FILIP LUCIAN SIMION and his identified

[4] This document replaces a lost, stolen, or destroyed national identification card in Belgium and must be obtained in person from a police station.

associates, LEONARDO CRISTEA, YMAN DJAVATKHANOV, ANDY NESTOR, and others.

28. On May 11, 2015, the FGP obtained a judicial order for telephone wiretaps of persons living in Belgium. It appears based on wire interceptions that members of the organization use “working phones” to contact each other, but rarely have conversations on the phones, only texting short messages or briefly talking in code. Investigators have noticed that communication on these “working phones” is often silent for days. For example, on October 7, 2015, investigators intercepted a SMS text message from NESTOR to SIMION stating, “Hi im here now can u call me on red.” On numerous other occasions in October and early November, NESTOR sent single SMS texts from his phone which stated, “Call red” or “Call on red.” FGP investigators and your affiant know that “red” means RedPhone. RedPhone was an app that enabled encrypted voice communications via internet. Based on this, coupled with activities observed by police on surveillance, the FGP believes that the members of the organization primarily use internet communication apps and encrypted email for substantive communications.

29. During the summer of 2015, FGP investigators and other police authorities observed SIMION and his suspected drug trafficking associates engaged in suspicious travel and meetings with each other, making circuitous trips that a reasonable person would not make to go from one destination to another and traveling long distances and across EU borders to meet someone for 5 or 10 minutes in a public location. Investigators determined that SIMION, who is a dual Belgian/Romanian citizen, and CRISTEA, a Romanian citizen, live in Bucharest, Romania, and NESTOR and DJAVATKHANOV are Belgian citizens living in Bruges, Belgium. The investigation

revealed that SIMION subsisted almost entirely on cash and frequently resided in hotels.

30. Between August 20, 2015, and September 3, 2015, FGP investigators determined that NESTOR and DJAVATKHANOV made several trips by car to the border areas of France and Germany. On September 4, 2015, the day after NESTOR and DJAVATKHANOV had driven into France, French police intercepted and seized four parcels from the mail addressed to different destinations in the U.S., each containing approximately 250 grams of MDMA. On September 7, 2015, French police intercepted two similar parcels containing MDMA and also bound for the U.S.

31. On September 16, 2015, FGP investigators observed ANDY NESTOR travel with an unknown female to company called “Storopack Packing Distribution Benelux NV” in Machelen, Belgium, where he purchased packaging materials, including mailing boxes and large padded envelopes.

32. On September 19, 2015, FGP investigators determined that ANDY NESTOR traveled to the Netherlands from Bruges, and they intercepted NESTOR on his cell phone asking an individual to pick up a backpack for him at the Bruges train station and take it to the Footlocker store where the individual worked. On September 20, 2015, investigators observed NESTOR pick up the backpack at the Footlocker.

33. On September 22, 2015, around 3:30 p.m., FGP investigators intercepted telephone calls of NESTOR’s during which they heard “hacking-knocking” sounds in the background. Based on their training and experience, investigators believe the sound was of someone cutting or preparing drugs. Later that evening, investigators observed NESTOR and DJAVATKHANOV drive together to France where they were observed

mailing four parcels. French authorities recovered the parcels, and each contained between 256 and 320 grams of MDMA. Three parcels were addressed to destinations in the U.S., and one parcel was bound for Canada. The packaging and invoices included in the parcels mirrored those previously identified as being used by IMB. In particular, the reverse side of two of the parcels had the address "36 Rue Damremont, 75018 Paris, France," the same return address as the parcel the HSI UC received from IMB on October 6, 2015. In addition, the interior of the parcels had black moisture barrier bags (MBB) with the label "Rough Orange Calcite" affixed to the MBB bags and an invoice. The invoices were labeled as from "Crystalitas Spiritual Community" and stated that the orders contained "ROUGH ORANGE CALCITE 250Grams." The packaging and invoices were nearly identical to those included in the parcel the HSI UC ordered and received from IMB.

34. Between October 9, 2015, and November 13, 2015, French police intercepted and seized 31 parcels from the mail in France, with each parcel containing between 64 grams and 378 grams of MDMA, most containing around 260 grams. All of the parcels were addressed to destinations in the U.S. One of the parcels, seized on October 21, 2015, and containing 260 grams of MDMA, was positively identified as a DEA Chicago undercover purchase from IMB.

35. On October 16, 2015, FGP investigators identified a garage rented by ANDY NESTOR at Wagenmakerstraat 27 8310 Bruges, Belgium since October 24, 2014. Between November 14, 2015 and March 15, 2016, investigators have observed CRISTEA, NESTOR, DJAVATKHANOV, and others coming and going from the garage, sometimes in the middle of the night and carrying backpacks or bags. Investigators

observed that on occasion the backpacks appeared to be full when entering the garage and empty when leaving. On other occasions, investigators observed that the backpacks appeared empty going in and full going out of the garage.

36. Based on the substance and patterns of conversations and call alerts intercepted, the FGP and your affiant believe that SIMION is running the drug trafficking organization. For example, on July 5, 2015, CRISTEA traveled from Romania to Belgium to meet SIMION, who was staying in Amsterdam, and DJAVATKHANOV, NESTOR, and others, who were located in Belgium. Upon CRISTEA's arrival, SIMION directed DJAVATKHANOV to drive CRISTEA to a hotel in the Netherlands, pay for the room, give CRISTEA spending money, and to buy CRISTEA a cheap mobile phone with a particular type of SIM card to use. In addition, on February 10, 2016, investigators intercepted phone conversations between YMAN DJAVATKHANOV and ANDY NESTOR regarding SIMION, whom they referred to as "the other one." During the conversations, NESTOR reported that "the other one" was unhappy that NESTOR did not answer his phone and return missed calls in a timely manner. NESTOR reported that SIMION was convinced they "couldn't reach a target" and asked them to drive. NESTOR told DJAVATKHANOV that he needed to come to his garage to talk to "the other one" (by phone). DJAVATKHAVOV sighed repeatedly, replying, "ok, yes.....problems again, dude, yes, I will come to your warehouse." Later, investigators observed DJAVATKHANOV meet NESTOR at the warehouse.

37. The following day, investigators observed NESTOR at the Wagenmakerstraat garage at approximately 9:42 a.m. While inside the garage, NESTOR called an individual to get the password to the "work computer." At 10:21 a.m., investigators

observed NESTOR leave the garage carrying a large envelope similar to the ones used for shipping drug parcels. An hour later, NESTOR called DJAVATKHANOV about taking a road trip.

38. On February 12, 2016, at 2:17 a.m., NESTOR called an individual about purchasing a Thalys (high speed train) ticket with the individual's credit card in exchange for cash. At 6:45 a.m., location data for NESTOR's and DJAVATKHANOV's phones indicated that they left the region of their homes in Bruges in the direction of the Belgium-Germany border via Brussels. From 10:31 a.m. to 1:30 p.m., their phones were outside of the Belgian cell phone networks. The location data indicated that they returned to Bruges via the same path at 4:10 p.m.

39. On March 10, 2016, at approximately 8:00 a.m., FGP investigators observed ANDY NESTOR and LEONARDO CRISTEA enter the garage at Wagenmakerstraat 27 in Bruges. NESTOR carried a large backpack, and CRISTEA carried a large envelope. Using a court authorized listening device located inside the garage, investigators heard and recorded conversations between NESTOR and CRISTEA. While inside, one of the men stated, "I'm going to call him now . . . Simion." After this, investigators heard NESTOR talking to someone over a phone or voice app, presumably SIMION. During the course of that conversation, NESTOR discussed the password for a computer in the garage, needing to get the computer repaired, and numerical quantities which investigators believe correspond to drug amounts and weights. Investigators believe that SIMION was giving instructions to NESTOR and CRISTEA regarding the preparation of MDMA orders. Approximately forty minutes after their arrival, NESTOR and CRISTEA continued to talk to each other while they prepared and packaged drugs,

with NESTOR giving specific instructions to CRISTEA about splitting, crushing and packaging the substances, keeping track of the amounts and number of pills being prepared. While this occurred, investigators could also hear several distinct sounds in the background: the rustling of paper and plastic material, typing on a computer keyboard, and the same "hacking-chopping" sounds they had previously heard over phone interceptions indicative of cutting and preparing MDMA. This activity and conversation continued for about an hour before NESTOR and CRISTEA left the garage; neither of them carried anything out.

40. The FGP has noticed during their investigation that most communications between the DTO members are conducted via device-based apps, such as RedPhone, Wickr, WhatsApp, and Signal, which investigators cannot intercept. Investigators advised that they noticed a pattern of activity occurring between the associates on a regular basis. First, police would intercept a short incoming call with no audio to the "working phones" in Belgium from phones which investigators believe are being used by SIMION. Investigators believe that this triggers communications between SIMION and the others via device-based apps or encrypted email. Shortly after these "triggering calls" would come in from SIMION to the "working phones" in Belgium, investigators would observe activity of CRISTEA, NESTOR, DJAVATKHANOV, and others indicative of filling and mailing drug orders, as described in paragraphs above. Confirming this, on March 10, 2016, FGP investigators recorded NESTOR say to CRISTEA in the Wagenmakerstraat garage, "He [SIMION] just called me on Signal, not on regular phone, that's why you don't hear. He always say me, 'first call on the normal phone and then on the Signal because otherwise I don't hear he does the Signal.'"

CONCLUSION

41. Based on the foregoing affidavit, there is probable cause to believe that FILIP LUCIAN SIMION, LEONARDO CRISTEA, YMRAN DJAVATKHANOV, and ANDY NESTOR have violated federal law, namely, Title 21, United States Code, Sections 846 and 963, conspiracy to distribute and import into the United States, from a place outside thereof, 3,4-methylenedioxy-methamphetamine (MDMA), a Schedule I controlled substance; therefore, your affiant respectfully requests that the Court issue warrants for their arrests.

42. I, Ryder K. Wells, being duly sworn according to law, hereby state that the facts in the foregoing amended affidavit are true and correct to the best of my knowledge, information and belief.

s/ Ryder K. Wells
Ryder K. Wells, Special Agent
Homeland Security Investigations

Submitted, attested to, and acknowledged by reliable electronic means on
March 16, 2016.

Nina Y. Wang
NINA Y. WANG
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF COLORADO

This Amended Complaint and Affidavit was reviewed and submitted by AUSA Michele R. Korver