UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
OCALA DIVISION

UNITED STATES OF AMERICA

v. CASE NO. 5:19-cr-5-Oc-28PRL

JUSTIN LEWIS

UNITED STATES' RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS EVIDENCE (DOC. 14)

The United States of America, by Maria Chapa Lopez, United States Attorney for the Middle District of Florida, through the undersigned Assistant United States Attorney, responds in opposition to defendant Justin Lewis's motion to suppress evidence obtained from a series of federal search warrants and orders to produce electronic evidence pursuant to 18 § U.S.C. 2703(d). Doc. 14.

SUMMARY

On June 26, 2018, the defendant, Justin Lewis, was indicted in the Northern District of Florida for nine counts of Wire Fraud, in violation of 18 U.S.C. § 1343, and one count of Aggravated Identity Theft, in violation of 18 U.S.C. § 1028(a)(1). NDFL Case No. 1:18-cr-15-GJ/MW. On February 6, 2019, Lewis was indicted in the Middle District of Florida for one count of Possession of Child Pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B).

Both the Northern and Middle District cases remain ongoing. On October 15, 2018, the defendant filed a motion to suppress seeking to exclude the evidence which resulted from one order issued pursuant to 18 U.S.C. § 2703(d) and twelve search warrants. The defendant asserts that the 2703 order and the warrants were defective, as well as claiming that the more recent warrants were based on impermissibly obtained information from prior warrants. The Government asserts that the warrants and order were properly obtained and valid.

TIMELINE OF 2703 ORDERS AND WARRANTS

In August of 2017, the Federal Bureau of Investigation (FBI) opened the investigation which led to the wire fraud charges against the defendant. During the course of the investigation, FBI agents applied for three orders issued pursuant to 18 U.S.C. § 2703(d) and twelve search warrants. The United States has summarized the orders and warrants that were obtained, categorizing them by reference to the defense exhibits described below:

Exhibit	Date	Subject	Type	Case Number
Ex A	8/16/2017	Verizon	2703 order	1:17-mc-7
Ex E	8/25/2017	Ebay1	2703 order	1:17-mc-22
Ex B	9/29/2017	Google	warrant	1:17-mj-47-GRJ
Ex C	2/6/2018	Residence (13280 SW 61st Place Road, Ocala, FL)	warrant	5:18-mj-1008-PRL
N/A	4/19/2018	Ebay2	2703 order	1:18-mc-3
Ex D	6/22/2018	iPad (1)	warrant	5:18-mj-1058-PRL
Ex D	6/22/2018	Western Digital Hard Drive	warrant	5:18-mj-1059-PRL
Ex D	6/22/2018	Laptop	warrant	5:18-mj-1060-PRL
Ex D	6/22/2018	Asus F3T Notebook	warrant	5:18-mj-1061-PRL
Ex D	6/22/2018	NXT Phantom 410 CPU	warrant	5:18-mj-1062-PRL
Ex D	6/22/2018	iPad (2)	warrant	5:18-mj-1063-PRL
Ex D	6/22/2018	Asus Laptop	warrant	5:18-mj-1064-PRL
Ex D	6/22/2018	Black iPhone	warrant	5:18-mj-1065-PRL
Ex D	6/22/2018	Silver iPhone	warrant	5:18-mj-1066-PRL
Ex D	6/22/2018	Antec computer	warrant	5:18-mj-1067-PRL

A single exhibit, Exhibit D, was attached by the defense for the warrants issued on June 22, 2018, because each of those warrants shared the same master affidavit.

The defendant is challenging the 2703(d) order issued on August 16, 2017 (Ex. A); the search warrant to obtain information from Google issued on September 29, 2017 (Ex. B); the search warrant for the defendant's residence at 13280 SW 61st Place Road, Ocala, Florida issued on February 6, 2018 (Ex. C); and the warrants issued on June 22, 2018, for ten devices recovered from the residence (Ex. D). The defendant references the two 2703(d) orders issued to eBay in his motion (although the defense motion erroneously refers to these as "search warrants") but does not appear to seek suppression of the information obtained from those orders.

FACTS

The FBI opened this case following a referral on August 16, 2017, from a representative from a credit union based on Cragislist and Ebay listings offering unlimited data on Verizon jetpack devices. The listings contained telephone number (727) 279-0008 as a contact number. The credit union representative did not identify the credit union customer by name, but indicated that large amounts of money were going through the customer's personal account. The

FBI referred the information to Verizon, who responded that, based on the phone number in the listings, they connected the information to Justin Lewis. Verizon reported that Lewis was the subject of a multi-million dollar fraud that Verizon had been dealing with internally. The FBI contacted the credit union and provided the name Justin Lewis. The credit union confirmed Lewis was their customer. Based upon the statements by the credit union representative and the internal work done by Verizon, it was believed that Lewis was connected to the listed telephone number. Based on this initial information, grand jury subpoenas were issued, and on August 16, 2017, the Government sought a 2703(d) order to obtain information from Verizon. (Ex. A.)

The FBI began receiving information from its subpoenas, as well as information from Verizon regarding their internal investigation. The FBI also began capturing screen shots from publicly available websites, as well as doing research on the companies and properties of the defendant and his mother.

On August 25, 2017, the FBI also sought information from eBay through a 2703(d) order regarding accounts associated with the defendant, his mother, and known emails and phone numbers associated with them. (Ex. E.) The 2703(d) order revealed that the defendant had three eBay accounts, one of

which was selling smart phones, and the defendant's mother had six accounts, one of which was advertising the sale of unlimited data plans.

During the investigation, the FBI received information from Verizon regarding the fraud. In particular, Verizon provided a copy of a contract with Razor Repair dated September 15, 2015, which listed the defendant as the owner (under Customer's Authorized Contacts) and the email as "JUSLEW352@gmail.com." Verizon also provided a copy of a contract with Page Plus Unlimited dated November 20, 2015, and listing the defendant as the owner (under Customer's Authorized Contacts), listing the company address as 13280 SW 61st Place Road, Ocala, Florida 34481, and the email as "juslew352@gmail.com." Both contracts, which were electronically signed by the defendant, state in paragraph 10:

No Reselling or Purchases by Third Parties: This Agreement specifically contemplates the purchase of Wireless Service by Corporate Subscribers and Employee Subscribers of Customer and Customer's qualifying parents and affiliates only as well as M2M Lines for Customer's business needs. Except upon written agreement between the Parties, third parties (including agents, contractors or contract employees, and members or franchisees of Customer or of Customer's qualifying parents and affiliates) may not purchase Wireless

Service or Equipment under this Agreement nor *may Customer resell the Wireless Service or use M2M Lines bundled with or embedded into products or services that it sells to its customers.*

(emphasis added).

Verizon also provided January 13, 2017, letters to the defendant and his mother where they indicated they would be cancelling the accounts due to the reselling activities. The defendant then sent emails to Verizon using the juslew352@gmail.com account which contained false statements in an effort to stall or prevent the cancellation of the accounts.

The FBI also learned that phone number (727) 279-0008 listed as a contact number in the eBay advertisements and the reselling website was associated with the defendant's mother's gmail account as a Google Voice number.

On September 29, 2017, based on the use of the email and the telephone number, the FBI sought and obtained a search warrant for the juslew352@gmail.com email account and the Google Voice account associated with (727) 279-0008. (Ex. B.)

Through the information obtained from the warrant for the juslew352@gmail.com email account, the FBI also learned that, following

Verizon's identification of him as an illegal reseller, the defendant was seeking to create or purchase companies (International Technology Solutions, Liberty Medical Management, and Paxton Industries) in the names of his associates, so he could continue his reselling activities. Furthermore, e-mails obtained via the search of juslew352@gmail.com indicated that the defendant used or intended to use his residence as a location for the on-going fraud. For example-

(1) an agreement indicating that International Technology Solutions mail should be delivered to the defendant's residence;

(2) a Registered Agent Services Agreement involving International Technology Solutions with the defendant's residence as the address;

(3) an agreement indicating that Liberty Medical Management mail should be delivered to the defendant's address;

(4) a Commercial Office Lease Agreement involving Paxton Industries with the defendant's address;

(5) a "Member Enrollment Agreement for Wireless Services" between Sprint Solutions, Inc. and Page Plus Unlimited where Page Plus Unlimited's operating address was the defendant's residence;

(6) a similar agreement between AT&T and Page Plus Unlimited where Page Plus Unlimited used the defendant's address;

(7) Verizon Wireless bills using defendant's address; and

(8) other bills for telecommunications accounts from E-Wireless Communications in Los Angeles, CA, where the defendant's address was used.

Based on the information that the defendant was involved in defrauding Verizon through the resale of their lines, and information that the defendant was using his residence in association with that business, the FBI then sought and obtained a search warrant on February 6, 2018, for the defendant's residence. The warrant sought records concerning the fraudulent activities in both physical and electronic form, and provided for search of electronic devices found within the residence. (Ex. C.)

On February 7, 2018, the warrant was executed and multiple devices were seized, including two iPads, a Western Digital Hard Drive, three laptops, an NXT Phantom 410 CPU, two iPhones, and a desktop computer. The FBI found information on several of the seized items related to the fraud against Verizon.

The review process by the FBI involved electronic images being taken of the data on each of the items and then the data images were uploaded for investigative review. When the images are uploaded, a technician checks the upload for data corruption by viewing one or two sample videos to see if the upload worked properly. Videos are used because they are easily corrupted during the process and are a good indicator of whether the upload worked properly. During the sampling in this case, the technician viewed a file which appeared to contain child pornography. This information was relayed to the investigating agent who sought and obtained additional warrants to search the devices for child pornography. (Ex. D.) Child pornography was ultimately located on two of these devices, which is the basis of the instant prosecution.

ARGUMENT/MEMORANDUM OF LAW

2703 Order Standard

An order for information sought under the Electronic Communications Privacy Act, pursuant to 18 U.S.C. § 2703(d), "shall only issue if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the concerns of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

Search Warrant Standard

A search warrant obtained under Federal Rule of Criminal Procedure 41 must be issued by an authorized judge "if there is probable cause to search for and seize a person or property . . . ." Fed.R.Crim.P. 41(d)(1). The warrant must be seeking (1) evidence of a crime; (2) contraband, fruits of crime, or other items illegally possessed; (3) property designed for use, intended for use, or used in committing a crime; or (4) a person to be arrested or a person who is unlawfully restrained. Fed.R.Crim.P. 41(c).

A. Verizon 2703(d) order

The defendant first challenges the 2703(d) order issued to Verizon. The defendant claims that statements in the warrant regarding telephone number (727)-279-0008, the eBay advertisement, and the ownership of Razor Repair were false and invalidate the order.

First, the information provided by the Government in the 2703(d) was based on the information provided to it at that time by the credit union and Verizon. Both entities had identified the defendant as the party associated with the possible fraud concerning the offer in the eBay which was using telephone number (727)-279-0008. Verizon also had an agreement with Razor Repair who listed the defendant as the owner.

Second, although further investigation revealed that the phone number and business were in the name of the defendant's mother, it also revealed that the defendant is the party behind the use of each item in the fraud. The eBay account was properly attributed to the defendant's mother in the affidavit.

Third, a 2703(d) order only requires "specific and articulable facts showing that there are reasonable grounds to believe that" the information sought was relevant and material to an ongoing criminal investigation. In this case, the information set forth in the Government's application accurately indicated that it had reasonable grounds to believe, based on the best information it had at that time, that the defendant was involved in a scheme to commit wire fraud by illegally resell Verizon accounts.

B. Gmail search warrant

The Government properly obtained the warrant for the information relating to the juslew352@gmail.com Google gmail account and the Google Voice account associated with (727) 279-0008. A review of the warrant affidavit shows that it relies on evidence indicating that the defendant was reselling accounts he received from Verizon, that he was using gmail account juslew352@gmail.com in conjunction with those activities, and that the

telephone number was listed as the contact number for the advertisements for the reselling activities.

The defendant challenges the warrant claiming that certain specific details are wrong or that he disagrees with them. For example, the defendant claims that the address of Page Plus Unlimited is wrong. However, that is the address the defendant listed as the address for Page Plus Unlimited in the contract with Verizon. The defendant also argues points that do not detract from the Government's affidavit, such as his claim on page 12 of the defense motion that there was more than one archive of the website referred to by the Government. However, even if that is true, it does not detract from what the Government saw in the archive it viewed.

The defendant's motion consists of such factual disputes to which the Government would respond by asserting that, with the exception of the years listed in paragraphs 20 and 23,[1] the facts of the affidavit are correct. Moreover, the facts set forth in the affidavit more than establish probable cause to believe that the email account and the Google Voice number were being used as part of the scheme.

[1] Verizon identified Lewis as potential reseller in November of 2016, not 2015. Also, the Verizon letter was dated January 13, 2017, not 2016. Neither date error effects the probable cause of the affidavit.

C. Warrant to Search 13280 SW 61st Place Road, Ocala, Florida

The defendant also challenges the search of the defendant residence, re-iterating many of the same issues as well as raising new issues of the same type. The Government would note that it found two factual errors. First, in paragraph 12, it should read November 2016, not 2015. Second, in paragraph 13 where the affidavit states "Verizon identified eBay advertisements for unlimited Verizon data that they traced to Lewis through the listed telephone number in that advertisement," it should state that Verizon received the advertisements from the Government and, with no identification other than the listed telephone number, internally connected them to conduct involving the defendant. Additionally, the Government would concede that the conclusion in paragraph 50 that the records indicating the purchase of six Apple laptops may be erroneous. The statement was based on six of sixteen payments to PowerbookME from September 28, 2015, through March 22, 2017. Those six payments ranged from $684.52 to $1359.79. However, the Government has learned that PowerbookME is a website called Powerbook Medic which repairs and sells Apple parts and products, as well as computers. So, the purchases may have been for repairs and/or parts, as well.

Other than these issues, the Government asserts that its affidavit is accurate and provides much more than probable cause to support the search of the defendant's residence.

The defendant also claims in his motion that the Government should have obtained information about the IP addresses used in order to establish the use of his residence in the scheme. However, the Government is not required to use any particular type of evidence to establish probable cause. Because the affidavit has sufficient probable cause to link the illegal activity to the residence, it is sufficient to support the warrant.

Finally, in the subsequent section addressing the warrants to re-search the devices seized from the defendant's residence, the defendant appears to claim that the search of the residence is improper because it was overbroad and lacked particularity. However, the warrant was neither overbroad, nor did it lack the necessary particularity.

The Fourth Amendment requires that warrants "particularly describ(e) the place to be searched, and the persons or things to be seized." U.S.Const. amend. IV. This requirement is aimed at preventing "general, exploratory rummaging in a person's belongings." *Coolidge v. New Hampshire*, 403 U.S. 443, 467, 91 S.Ct. 2022, 2038, 29 L.Ed.2d 564 (1971); *see generally Stanford v. Texas*,

379 U.S. 476, 481-85, 85 S.Ct. 506, 509-511, 13 L.Ed.2d 431 (1965) (requirement of particular description derives from Colonial resistance to general warrants and writs of assistance); *United States v. Osborne*, 630 F.2d 374, 378 (5th Cir. 1980), cert. denied, 450 U.S. 934, 101 S.Ct. 1398, 67 L.Ed.2d 369 (1981). A description is sufficiently particular when it enables the searcher to reasonably ascertain and identify the things authorized to be seized. *United States v. Cook*, 657 F.2d 730, 733 (5th Cir. 1981), citing *Steele v. United States*, 267 U.S. 498, 503-04, 45 S.Ct. 414, 416-417, 69 L.Ed. 757 (1925). Failure to adequately enforce the particularity requirement would undermine the warrant requirement itself, and increase the risk of an excessive intrusion into the areas of personal rights protected by the Fourth Amendment. *Cook, supra*, 657 F.2d at 733 ("weigh the practical necessities of law enforcement against the likelihood of a violation of the personal rights of the one whose premises and possessions are to be searched").

At the same time, the Supreme Court has recognized that effective investigation of complex white-collar crimes may require the assembly of a "paper puzzle" from a large number of seemingly innocuous pieces of individual evidence: "The complexity of an illegal scheme may not be used as a shield to avoid detection when the State has demonstrated probable cause to

believe that a crime has been committed and probable cause to believe that evidence of this crime is in the suspect's possession." *Andresen v. Maryland*, 427 U.S. 463, 481 n.10, 96 S.Ct. 2737, 2749 n.10, 49 L.Ed.2d 627 (1976). *See also United States v. Jacob*, 657 F.2d 49, 52 (4th Cir. 1981) (consider complexity of alleged fraud), cert. denied, —- U.S. ——, 102 S.Ct. 1435, 71 L.Ed.2d 653 (1982); *United States v. Abrams*, 615 F.2d 541, 548 (1st Cir. 1980) (Campbell, J., concurring) (investigators in fraud cases do not and often cannot know in advance what precisely they will find in files). It is universally recognized that the particularity requirement must be applied with a practical margin of flexibility, depending on the type of property to be seized, and that a description of property will be acceptable if it is as specific as the circumstances and nature of activity under investigation permit. *United States v. Wuagneux*, 683 F.2d 1343, 1349 (11th Cir. 1982); (citing *United States v. Lowry*, 675 F.2d 593, 595 (4th Cir. 1982).

In the present case, which involves a complex financial investigation and widespread allegations of fraud, the warrant should be read with a practical flexibility and an awareness of the difficulty of piecing together the type of "paper puzzle" involved in this case. *See United States v. Wuagneux*, 683 F.2d at 1349. As such, because the warrant limited itself to records involved in the

fraud (both paper and electronic) and the type of records which would be evidence of the fraud, it is not overbroad.

D. Warrants to Re-search Devices for Child Pornography

The defendant finally challenges the second search of his devices for child pornography. The defendant does not challenge the accuracy of the affidavit submitted for the devices. Instead, he claims that it is based on invalid prior warrants, and should be suppressed as "fruit of the poisonous tree." However, as set forth above, all prior 2703(d) orders and warrants were properly obtained, so there is no basis to the defendant's claim that the second search of the devices from defendant's residence is based on evidence improperly obtained.

Good Faith Exception

In *United States v. Leon*, 468 U.S. 897, 922-23 (1984), the Supreme Court held that the Fourth Amendment exclusionary rule should not be applied to exclude the use of evidence obtained by officers acting in reasonable reliance on a detached and neutral magistrate judge's determination of probable cause in the issuance of a search warrant that is ultimately found to be invalid. The officer's reliance on the magistrate judge's probable cause determination must be objectively reasonable.

Four circumstances, none of which are present here, exist in which the *Leon* good faith exception does not apply and suppression remains an appropriate remedy: (1) the magistrate judge issuing the warrant was misled by statements made by the affiant that were false or made in "reckless disregard for the truth;" (2) "the issuing magistrate wholly abandoned his [or her] judicial role;" (3) the affidavit in support of the warrant is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable;" or (4) the warrant is "so facially deficient . . . that the executing officers cannot reasonably presume it to be valid." *Id. at 9*23.

None of the circumstances which preclude reliance on *Leon* exist in this case. First, there is no allegation or any evidence that statements made by the affiant were false or made in reckless disregard for the truth. Second, there is no evidence that the judge in this case abandoned his judicial role in examining the affidavit. Third, sufficient probable cause is contained in support of the warrant to allow the officers to reasonably rely on it, based on the totality of the circumstances. Finally, the face of the warrant describes with sufficient particularity the place to be searched, and is not facially deficient.

The defendant argues that the *Leon* exception should not be applied because the officer who submitted the warrant was the same one who executed

it. The defendant cites to *Leon* for this proposition. However, *Leon* does not support the defendant's assertion. The defendant appears to be conflating the first circumstance listed above with the broader rule that he is attempting to assert. The rule prohibits use of the good faith exception when there is evidence that the magistrate judge issuing the warrant was misled by statements made by the affiant that were false or made in "reckless disregard for the truth." The defendant appears to be arguing that such circumstances would exist in every case where the warrant is executed by the affiant. However, such is not the case and *Leon* can apply where an affiant also executes the warrant so long as the affiant did not make statements which were false or made in "reckless disregard for the truth."

Because the agent in this case did not act in "reckless disregard for the truth," *Leon* is applicable, and the agents were entitled to rely on their good faith belief in the validity of the warrants they obtained.

CONCLUSION

For all the foregoing reasons, the Court should deny defendant Lewis's motion to suppress evidence in its entirety.

Respectfully submitted,

MARIA CHAPA LOPEZ
United States Attorney

By: *s/ William S. Hamilton*
William S. Hamilton
Assistant United States Attorney
Florida Bar No. 95045
35 SE 1st Avenue, Suite 300
Ocala, Florida 34471
Telephone: (352) 547-3600
Facsimile: (352) 547-3623
E-mail: william.s.hamilton@usdoj.gov

U.S. v. JUSTIN LEWIS **Case No. 5:19-cr-5-Oc-28PRL**

CERTIFICATE OF SERVICE

I hereby certify that on March 29, 2019, I electronically filed the foregoing with the Clerk of the Court by using the CM/ECF system which will send a notice of electronic filing to the following:

Jack Maro, Esq.

s/ William S. Hamilton
William S. Hamilton
Assistant United States Attorney
Florida Bar No. 95045
35 SE 1st Avenue, Suite 300
Ocala, Florida 34471
Telephone: (352) 547-3600
Facsimile: (352) 547-3623
E-mail:william.s.hamilton@usdoj.gov