APPENDIX TABLE OF CONTENTS

OPINIONS AND ORDERS

REHEARING ORDER

OTHER DOCUMENTS

OPINION OF THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT (MARCH 28, 2022)

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

FOR PUBLICATION

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

VOLODYMYR KVASHUK,

Defendant-Appellant.

No. 20-30251

D.C. No. 2:19-cr-00143-JLR-1

Appeal from the United States District Court
for the Western District of Washington
James L. Robart, District Judge, Presiding

Before: Richard A. PAEZ, Milan D. SMITH, JR.,
and Jacqueline H. NGUYEN, Circuit Judges.

NGUYEN, Circuit Judge:

Volodymyr Kvashuk stole $10 million in digital gift cards from his employer, Microsoft, using login credentials he filched from his coworkers. Microsoft

uncovered Kvashuk's scheme and fired him after noticing unusual gift card redemption activity.

Unbeknownst to Kvashuk, Microsoft also referred the matter to law enforcement. Over the next 13 months, the Internal Revenue Service ("IRS") investigated both the gift card theft and Kvashuk's failure to report the illegal income on his tax returns. Government agents recovered additional evidence when they executed a search warrant on Kvashuk's home and vehicle.

In this appeal from his conviction for 18 fraud-related counts, Kvashuk contends that: the search warrant lacked probable cause; his coworkers' login credentials were not a "means of identification," 18 U.S.C. § 1028A(a)(1); the exclusion of evidence that he had applied for asylum prevented him from presenting a complete defense; and the district court should have dismissed a juror who worked for the same team at Microsoft. None of these contentions has merit. Therefore, we affirm the district court's judgment.

I. Background

A. Kvashuk's Employment at Microsoft

Kvashuk grew up in Ukraine and came to the United States in 2015 at age 21. In August 2016 he landed his first job in the tech industry as a software engineer at Microsoft's Redmond, Washington campus. For roughly the first year, he worked as a contractor, and after a two-month hiatus, he returned to Microsoft as a direct employee in December 2017.

Kvashuk worked on various projects involving the user experience at the Universal Store. The Universal Store is Microsoft's online portal for selling computer

hardware, television shows, movies, games, and applications. It is universally available on devices running a Microsoft operating system, such as a Windows PC, an Xbox game console, or a Windows phone, but anyone with access to the internet and an email address can create an account and place an order.

Software engineers working on the Universal Store team ("UST") wrote and tested code. Most testing was performed "in production"—*i.e.*, using the code version that an end user would experience. UST members tested the steps that a user would go through to purchase a product at the Universal Store—the user's "purchase flow"—by creating test accounts. Test accounts were the same as any other Universal Store account, with three main exceptions.

First, the email addresses used for test accounts started with "mstest_" followed by an alias selected by the individual tester. For example, Kvashuk's test account was mstest_v-vokvas@outlook.com.

Second, Microsoft provided UST members with special credit cards ("test-in-production" or "TIP" cards) for use with the test accounts. TIP cards were not real credit cards—no bank would honor them—but the Universal Store accepted the cards as a means of payment without submitting the transaction to a bank for processing. Thus, TIP cards allowed software engineers to test the Universal Store purchase flow without money changing hands.

Third, Microsoft suppressed the shipment of any physical goods ordered from a test account. Crucially, however, this safeguard did not apply to digital gift cards delivered via email.

A digital gift card is a token—a 25-character code broken into five groups of five characters separated by hyphens—that can be redeemed for a specified amount of credit ("currency stored value" or "CSV") at the Universal Store. A digital gift card purchaser need not redeem the token herself; anyone with a Universal Store account can redeem it.

B. Microsoft's Investigation

In February 2018, Microsoft's fraud investigation strike team ("FIST") noticed a suspicious spike in Xbox Live subscriptions paid for with CSV. The FIST traced the CSV to tokens ordered through two test accounts: mstest_sfwe2eauto@outlook.com, which belonged to UST member Andre Chen, and mstest_avestu@outlook.com, which belonged to UST member Roy Morey.

Microsoft suspended these two test accounts on March 15, 2018, and cancelled any unredeemed tokens purchased through them. At the time, the FIST believed that an outside actor had ordered the tokens because the IP addresses associated with the transactions were external to Microsoft,[1] and the FIST investigator who interviewed Chen and Morey did not suspect their involvement.

On March 22, 2018, the FIST noticed another spike in CSV purchases traceable to a third test account: mstest_zabeerj2@outlook.com, which belonged to UST member Zabeer Jainullabudeen. These transactions were made from a device using the same hosting IP company as the transactions that originated from the

[1] An Internet Protocol ("IP") address is a numerical label assigned to each device that is connected to a computer network that accesses the internet.

sfwe2eauto and avestu test accounts. The next day, Microsoft suspended the zabeerj2 test account and cancelled the unredeemed tokens purchased through it. In all, $10 million worth of tokens was stolen through the three test accounts, and Microsoft cancelled only $1.8 million worth before the tokens were redeemed for CSV, resulting in a loss to the company of approximately $8.2 million.

Microsoft came to suspect Kvashuk when the FIST searched for other accounts that had accessed the Universal Store from the IP addresses used to steal CSV. Multiple IP addresses associated with the sfwe2eauto or avestu test accounts were also associated with Kvashuk's v-vokvas test account, his personal Outlook account (safirion@outlook.com), and his personal Gmail account,[2] as well as an additional account: pikimajado @tinoza.org.

Kvashuk's v-vokvas test account, the pikimajado account, and another account—xidijenizo@axsup.net—were also linked to the sfwe2eauto and avestu test accounts through the same "fuzzy device ID." A fuzzy device ID is a "fairly unique" identifier generated by Microsoft—a string of information that identifies characteristics about the user's browser, operating system, and other attributes. According to Microsoft, it is "theoretically possible" but "very unlikely" that two different devices would have the same fuzzy device ID.

---

[2] Microsoft knew Kvashuk's personal Gmail account from his resume. Microsoft deduced that the safirion account belonged to Kvashuk because the name on the account was "volo kv" (*i.e.*, the first few letters of Kvashuk's first and last names) and one of the mailing addresses for the account was the apartment where Kvashuk lived until April 2018.

Microsoft discovered that in October 2017, Kvashuk's v-vokvas test account ordered a single token that another account, linked to an email address at searchdom.io, redeemed for a subscription to Microsoft Office. Kvashuk was a registered owner of searchdom.io. Two weeks later, the v-vokvas test account ordered tokens worth approximately $10,000, of which approximately $2,500 was redeemed for CSV in the Universal Store by accounts linked to the pikimajado and xidijenizo email accounts. These two accounts used the CSV to purchase graphics cards and ship them to "Grigor Shikor" at Kvashuk's apartment complex.

In two interviews, Kvashuk admitted to Microsoft investigators that he had used his test account to generate tokens, which he claimed he redeemed to watch movies. He also admitted purchasing a graphics card on the Universal Store using CSV he obtained from the test account. He claimed that he had wanted to see whether it was possible to order physical items that way but that the graphics card never arrived.[3] When asked if he knew Grigor Shikor, Kvashuk first told the investigators, "It's complicated," and then denied knowing him.

Microsoft terminated Kvashuk's employment in June 2018 and informed the Department of Justice about the stolen CSV.

---

[3] Evidence in the record suggests that the graphics card was indeed delivered to Kvashuk's apartment complex even though the specific apartment number to which it was shipped did not exist.

C. Kvashuk's Criminal Prosecution

The government learned additional details through its investigation. The name on Kvashuk's phone account was Grigory Kvashuk. Many of the IP addresses Kvashuk used to access the Universal Store belonged to a company operating a virtual private network ("VPN").[4]

Kvashuk also had sudden, unexplained wealth. His salary at Microsoft was $116,000, and his bank account at Wells Fargo had a balance of less than $20,000 until late November 2017. Between November 2017 and May 2018, Kvashuk transferred over $2.8 million from a cryptocurrency account he held at Coinbase.com into his bank account. By examining the Bitcoin blockchain (a public ledger of Bitcoin transactions), the government determined that the Bitcoin deposits in Kvashuk's Coinbase account came from a mixing service, which obscures the Bitcoin's source by mixing potentially identifiable Bitcoin with other Bitcoin. Kvashuk used the cash from his Coinbase account to purchase a $162,000 Tesla Model S in March 2018 and, three

---

[4] When an internet user connects to a website via a VPN, it will appear to the website (which may be recording the user's IP address) that the user is connecting via the VPN's IP address rather than the IP address of the device where the user is located. Thus, a VPN is a tool that provides a degree of privacy. It has many legitimate uses, such as securing corporate data, preventing advertisers from collecting personal information, and avoiding suppression and censorship by foreign governments. A VPN can also be used by criminals to conceal their involvement in cybercrime, as the government argued Kvashuk did here. Many Microsoft employees used the same VPN as Kvashuk. The VPN assigned non-unique IP addresses; more than 100 users could share one of its IP addresses at any given time.

months later, a $1.675 million house on the shore of Lake Washington.

Through a search warrant served on Google, the government obtained Kvashuk's Gmail messages and internet search history and learned that Kvashuk had been selling the stolen tokens on a Paxful account. Paxful.com is a peer-to-peer Bitcoin marketplace that allows users to exchange Bitcoin for gift cards, among other things. Kvashuk's chats on Paxful with purchasers of the gift card tokens revealed that he received 55 to 60 cents worth of Bitcoin for every dollar of CSV that he sold.

The government subsequently executed a search warrant on Kvashuk's lakefront house and car and seized additional evidence tying Kvashuk to the stolen CSV. Kvashuk was indicted on 18 fraud-related counts, including two counts of aggravated identity theft, 18 U.S.C. § 1028A.[5]

Prior to trial, the district court denied Kvashuk's motions to suppress the evidence obtained from his house and car and to dismiss the aggravated identity theft counts for failure to state an offense. Over Kvashuk's objection, the court granted in part the government's motion in limine to exclude evidence that Kvashuk had applied for asylum—in particular, a statement that he made to his tax preparer regarding his

---

[5] In addition, the indictment charged Kvashuk with one count of access device fraud, 18 U.S.C. § 1029(a)(5), (c)(1)(A)(ii); one count of access to a protected computer in furtherance of fraud, *id.* § 1030(a)(4), (c)(3)(A); one count of mail fraud, *id.* § 1341; five counts of wire fraud, *id.* § 1343; two counts of filing a false tax return, 26 U.S.C. § 7206(1); and six counts of money laundering, 18 U.S.C. § 1957.

immigration status. At trial, when a juror disclosed that he had worked on the UST during the two years before Kvashuk began working at Microsoft, Kvashuk unsuccessfully moved to dismiss the juror.

The jury convicted Kvashuk of all counts. Kvashuk moved for judgment of acquittal on the aggravated identity theft counts due to insufficient evidence. In addition, he moved for a new trial because the court excluded evidence of his asylum application and declined to dismiss the juror with UST experience. The district court denied both motions and sentenced Kvashuk to nine years in prison. We have jurisdiction under 28 U.S.C. § 1291.

II. Discussion

A. Motion to Suppress Evidence Seized from Kvashuk's House

Kvashuk challenges the denial of his motion to suppress evidence seized from his house on the ground that the search warrant lacked probable cause.[6] Relatedly, he challenges the district court's denial of his request for a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978).

We review the district court's denial of a motion to suppress de novo and any underlying factual findings for clear error. *United States v. Kleinman*, 880

---

[6] Kvashuk also challenges the search of his car, but the only evidence from the car introduced at trial was Kvashuk's employee badge. Since it was undisputed that Kvashuk worked at Microsoft, and the evidence had no other significance, any error from the district court's refusal to suppress it was harmless beyond a reasonable doubt. *See United States v. Job*, 871 F.3d 852, 865 (9th Cir. 2017).

F.3d 1020, 1036 (9th Cir. 2017). The district court's denial of a request for a *Franks* hearing is also reviewed de novo. *Id.* at 1038.

1. Nexus between the scheme and the place to be searched

"A warrant must be supported by probable cause —meaning a 'fair probability that contraband or evidence of a crime will be found in a particular place based on the totality of circumstances.'" *United States v. King*, 985 F.3d 702, 707 (9th Cir. 2021) (quoting *United States v. Diaz*, 491 F.3d 1074, 1078 (9th Cir. 2007)). The magistrate's probable cause determination "should be paid great deference by reviewing courts." *Id.* (quoting *Illinois v. Gates*, 462 U.S. 213, 236 (1983)). Review "is limited to ensuring that the magistrate had a 'substantial basis' for concluding that probable cause existed." *Id.* at 708 (quoting *Gates*, 462 U.S. at 238).

Kvashuk does not dispute that there was probable cause to suspect him of crimes in connection with the stolen CSV. Rather, he argues that the warrant affidavit failed to "establish a nexus between the unlawful activities and the places to be searched."

It is true that "[p]robable cause to believe that a suspect has committed a crime is not by itself adequate to secure a search warrant for the suspect's home." *United States v. Ramos*, 923 F.2d 1346, 1351 (9th Cir. 1991), *overruled on other grounds by United States v. Ruiz*, 257 F.3d 1030, 1032 (9th Cir. 2001) (en banc). But "the nexus between the items to be seized and the place to be searched" can rest on "normal inferences as to where a criminal would be likely to hide" evidence of his crimes. *United States v. Spearman*, 532 F.2d 132,

133 (9th Cir. 1976) (per curiam) (quoting *United States v. Lucarz*, 430 F.2d 1051, 1055 (9th Cir. 1970)).

While we have not directly addressed the nexus issue, our cases confirm that the nature of cybercrime—specifically, its reliance on computers and personal electronic devices—is relevant to probable cause for searching the suspect's residence. *See United States v. Adjani*, 452 F.3d 1140, 1145 (9th Cir. 2006) (holding that evidence of the suspect's "extortion scheme . . .requiring the use of a computer" justified a search warrant for any computers found at the suspect's home); *United States v. Gourde*, 440 F.3d 1065, 1071 (9th Cir. 2006) (en banc) (holding that evidence the suspect maintained membership in a website with child pornography supported search of the computer at his residence); *see also United States v. Green*, 954 F.3d 1119, 1123 (8th Cir. 2020); *United States v. Jones*, 942 F.3d 634, 639–40 (4th Cir. 2019); *Peffer v. Stephens*, 880 F.3d 256, 272–73 (6th Cir. 2018); *United States v. Joubert*, 778 F.3d 247, 252–53 (1st Cir. 2015); *United States v. Watzman*, 486 F.3d 1004, 1007–08 (7th Cir. 2007).

Here, the warrant affidavit explained in detail how Kvashuk committed the suspected crimes "almost entirely via digital devices." Such devices "were used to access . . . Microsoft's online store, set up and access email accounts, conduct online research in furtherance of the scheme, purchase and redeem CSV, communicate with one or more tax preparers, and conduct bitcoin transactions." The affidavit also pointed out that "many people generally keep their cell phones and other digital devices . . . in their home" and provided extensive evidence that Kvashuk did so here. For example, the affidavit noted that (1) Kvashuk was a

software engineer; (2) his house had internet service; (3) the IP address assigned to his house was used in 2018 and 2019 to access his Coinbase and Gmail accounts, both of which were involved in his scheme;[7] (4) he emailed his tax preparer in February 2019 regarding the preparation of his false 2018 return; and (5) based on the affiant's training and experience, "people often keep personal, financial, and tax records in their home," including Bitcoin private keys (essentially, passwords necessary to control their Bitcoin). All of this evidence, taken together, was enough to reasonably establish a nexus between the digital devices to be seized and Kvashuk's home.

Kvashuk argues that "it is chronologically impossible for the theft at issue to be committed by way of a digital device inside the [lakefront] house" given that Microsoft disabled the test accounts before he moved there in April 2018. But this is irrelevant. "[P]robable cause to believe that a person conducts illegal activi-

---

[7] To the extent Kvashuk maintains that the search of his Gmail account lacked probable cause because he did not use it to purchase or redeem tokens, we disagree. In December 2017, Kvashuk accessed the Universal Store from an account linked to his Gmail account at least nine times, and accessed his Coinbase account once, from various IP addresses later used by the test accounts to steal CSV. Although other Microsoft employees used the same IP addresses, which belonged to a commercial VPN, Kvashuk was specifically linked to the stolen CSV transactions through the fuzzy device ID used to access his v-vokvas, pikimajado, and xidijenizo accounts. Moreover, Coinbase records showed communications with Kvashuk's Gmail account. The IRS agent who prepared the affidavit attested that such communications "may be evidence of financial transactions conducted using the proceeds of the fraud, and therefore be evidence of money laundering." And there was a clear pattern of deposits into Kvashuk's Coinbase account that followed redemption of the stolen CSV.

ties in the place where he is to be searched is not necessary; the proper inquiry is whether there was probable cause to believe that evidence of illegal activity would be found in the search." *United States v. Elliott*, 322 F.3d 710, 716 (9th Cir. 2003).

The affidavit contained evidence that the house had internet service and that the IP address associated with the house was used to access Kvashuk's Gmail and Coinbase accounts. It was thus reasonable for the magistrate to infer that Kvashuk brought his digital devices with him—including those used to perpetrate the theft—when he moved from the apartment to the house. *See United States v. Richardson*, 607 F.3d 357, 371 (4th Cir. 2010) (rejecting contention that "that there must be some 'specific' allegation that [the suspect] . . . was using the same computer at the new residence"). Moreover, Kvashuk's use of the test accounts to order digital gift cards was only the first step of his scheme, which continued until he transferred the proceeds from his Coinbase account into his Wells Fargo bank account. According to the affidavit, Kvashuk continued making these transfers through May 2018.

Considering "the totality of [the] circumstances," *King*, 985 F.3d at 707 (quoting *Diaz*, 491 F.3d at 1078), the search warrant affidavit shows a fair probability that evidence of Kvashuk's crimes would be found on a computer at his residence. Therefore, there was an adequate nexus between the unlawful activities and the place to be searched.

2. Staleness

Kvashuk asserts that the information in the search warrant affidavit was mostly stale, and thus did not support probable cause, because it involved

events that occurred more than a year before the search warrant was presented to the magistrate in July 2019. His staleness argument does not withstand scrutiny.

To be sure, "[t]he most convincing proof that [evidence of a crime] was in the possession of the person or upon the premises at some remote time in the past will not justify a present invasion of privacy." *United States v. Grant*, 682 F.3d 827, 832 (9th Cir. 2012) (quoting *Durham v. United States*, 403 F.2d 190, 193 (9th Cir. 1968)). But the "mere passage 'of substantial amounts of time is not controlling in a question of staleness.'" *United States v. Flores*, 802 F.3d 1028, 1043 (9th Cir. 2015) (quoting *United States v. Dozier*, 844 F.2d 701, 707 (9th Cir. 1988)).

"That is particularly true with electronic evidence." *Id.* Given "the long memory of computers," evidence of a crime typically remains on a computer even if the defendant attempts to delete it. *Id.* (quoting *Gourde*, 440 F.3d at 1071); *see Gourde*, 440 F.3d at 1068 (explaining that deleted files "were not actually erased but were kept in the computer's 'slack space' until randomly overwritten, making [them] retrievable by computer forensic experts").[8]

Here, as in *Gourde*, the affidavit supporting the search warrant explained that "computer files . . . can be preserved (and consequently also then recovered)

---

[8] "Of course, at some point 'after a *very* long time' the likelihood that certain digital information will be recoverable from a specific device 'drops to a level at which probable cause to search the suspect's home for the computer can no longer be established.'" *United States v. Rees*, 957 F.3d 761, 770 (7th Cir. 2020) (quoting (*United States v. Seiver*, 692 F.3d 774, 777 (7th Cir. 2012)). The timeframes in this case present no such issue.

for months or even years after they have been downloaded onto a storage medium, deleted, or accessed or viewed via the Internet," and that even after deletion, files often still reside in the computer's "slack space." Although most of the evidence of the CSV theft was 15–20 months old at the time of the warrant application, a temporal gap of that magnitude is not extreme relative to the lifespan of a computer. *See, e.g.*, *United States v. Schesso*, 730 F.3d 1040, 1047 (9th Cir. 2013) (holding that "a mere 20 months" was not too long to expect data to remain recoverable).

Kvashuk was unaware of the criminal investigation into his theft, so he had no reason to delete or encrypt any incriminating files. In fact, the warrant served on Google just two months earlier had yielded relevant evidence from Kvashuk's Gmail account and browser history. And the search warrant application sought not only evidence of the theft, but also evidence of Kvashuk's suspected false tax returns. He had communicated with his tax preparer in February 2019—five months before the search warrant application. The evidence supporting the application was not stale.

3. *Franks* hearing

"To obtain a *Franks* hearing, a defendant must make a substantial preliminary showing that: (1) 'the affiant officer intentionally or recklessly made false or misleading statements or omissions in support of the warrant,' and (2) 'the false or misleading statement or omission was material, *i.e.*, necessary to finding probable cause.'" *United States v. Norris*, 942 F.3d 902, 909–10 (9th Cir. 2019) (quoting *United States v. Perkins*, 850 F.3d 1109, 1116 (9th Cir. 2017)), *cert. denied*, 140 S. Ct. 2754 (2020). Kvashuk identifies no false or mis-

leading statement in the affidavit, let alone one that the affiant—lead IRS case agent Eric Hergert—made intentionally or recklessly.

That Hergert failed to note Kvashuk's claim to have changed his company's email domain from "searchdom.io" to "searchdom.ai" is inconsequential. There is no evidence that this change occurred before October 2017, when an account linked to the searchdom.io domain redeemed CSV obtained from the vokvas test account. Even if Searchdom had changed domains by then, there is also no evidence to support Kvashuk's theory that someone unconnected to his company was operating the searchdom.io email account. Indeed, when Microsoft investigated searchdom.io in March 2018 or later, Kvashuk was still listed as a registered owner. In May 2018, when the FIST asked Kvashuk who controlled the Searchdom domains, Kvashuk did not disclaim ownership of searchdom.io; to the contrary, he indicated that he had access to the Searchdom site generally.

Hergert's statement that Kvashuk "has a Samsung phone" and that "[l]ocation records received . . . often place this phone at the [lakeside house], including during evening hours," did not, as Kvashuk argues, imply that he "accessed the CSV codes or test account from his phone." Rather, it showed that Kvashuk lived at the house as early as April 2018, even though he did not own the house until two months later.

Nor was it misleading for Hergert to omit the statement he had earlier included in the Google search warrant affidavit that the government had "only limited evidence" regarding how Kvashuk sold the CSV and transferred the funds to his bank account. By the time the agents sought to search Kvashuk's

house, they had obtained substantial evidence regarding these financial transactions—much of it derived from the records obtained from Google.

B. Convictions for Aggravated Identity Theft

Kvashuk next challenges his convictions for aggravated identity theft, which stem from his use of Chen's swfe2eauto test account and Jainullabudeen's zabeerj2 test account. Kvashuk contends that these two convictions are infirm because the test accounts do not constitute a "means of identification." 18 U.S.C. § 1028A(a)(1). We review the district court's denial of a motion for judgment of acquittal de novo, "viewing the evidence in the light most favorable to the prosecution." *United States v. Charley*, 1 F.4th 637, 643 (9th Cir. 2021) (quoting *United States v. Vazquez-Hernandez*, 849 F.3d 1219, 1229 (9th Cir. 2017)).

Aggravated identity theft requires proof that the defendant, "during and in relation to" certain felonies,[9] "knowingly transfer[red], possesse[d], or use[d], without lawful authority, a means of identification of another person." 18 U.S.C. § 1028A(a)(1).

> [T]he term "means of identification" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any—
>
> (A) name, social security number, date of birth, official State or government issued driver's

[9] The underlying felonies here were access device fraud and access to a protected computer in furtherance of fraud, as charged in counts one and two, respectively. *See* 18 U.S.C. § 1028A(c)(4).

> license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
>
> (B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
>
> (C) unique electronic identification number, address, or routing code; or
>
> (D) telecommunication identifying information or access device. . . .

Id. § 1028(d)(7) (emphasis added).

Kvashuk argues that the test accounts do not "identify a specific individual," *id.*, because "they are simply tools for the testers to do their jobs for Microsoft." He points out that the test accounts serve "Microsoft's business purposes," "are strictly controlled by Microsoft," "are 'programmed' to make test purchases 'in an automated fashion,'" and have TIP cards "associated with [them], not with the individual testers."

The test accounts' purpose, prerequisites, and functionality do not bear on whether they "identify a specific individual." In drafting the statute, Congress intended "to construct an expansive definition" of the term "means of identification," *United States v. Alexander*, 725 F.3d 1117, 1121 (9th Cir. 2013) (quoting *United States v. Blixt*, 548 F.3d 882, 887 (9th Cir. 2008)), and "to protect businesses from financial loss," *United States v. Maciel-Alcala*, 612 F.3d 1092, 1100 (9th Cir. 2010).

The test accounts at issue here clearly could be used to identify specific Microsoft employees because

the company's investigators actually did identify four individuals—Chen, Morey, Jainullabudeen, and Kvashuk—as the owners of test accounts that had been used to purchase CSV. At oral argument, Kvashuk's counsel acknowledged that "every Microsoft employee has [a Microsoft] email address that is individual to him or her." That UST members use their Microsoft email accounts for certain business purposes (counsel gave the example of communicating with human resources) and their test email accounts for other business purposes makes no difference to whether the test email accounts identify specific testers. *See United States v. Barrington*, 648 F.3d 1178, 1192–93 (11th Cir. 2011) (rejecting argument that employee "passwords . . . used to access the [university's] computer system belonged to the university and do not constitute personal identity information of the individual university employees").

Kvashuk also argues that "the testers shared the login information of the test accounts among the team," and the credentials thus "identify a member of the testing team, but not the particular individuals." While rampant sharing of test account credentials among the testers could render the accounts unreliable as a means of identification, the evidence does not support that characterization of what occurred at Microsoft.

Testers "sometimes" shared test accounts and passwords, but Kvashuk's manager, Marshall Wilcox, told the testers that "they shouldn't be sharing," because it made the accounts "harder to trace individually." There were exceptions where Wilcox authorized password sharing to test specific purchase flows, but none of these exceptions involved Kvashuk, and Wilcox never gave Kvashuk permission to use a test account assigned to another employee.

In many organizations, individuals commonly allow someone else—an assistant, an IT professional, or even a colleague—to access their email account for specific, limited purposes. Because such an individual has primary control of the account and the account remains associated with his or her identity, the account still identifies the individual specifically and thus retains its status as "a means of identification." 18 U.S.C. § 1028A(a)(1). Here, the UST members' limited sharing of test accounts and passwords, both authorized and informal, was insufficient to differentiate the test accounts from any other business email account associated with a specific person. The district court properly denied Kvashuk's motion for judgment of acquittal.

C. Exclusion of Evidence of Kvashuk's Asylum Application

Kvashuk contends that the district court violated his due process rights by preventing him from presenting a complete defense. In particular, he argues that the court erred in excluding evidence of his status in the United States as an asylum applicant. "Generally, we review the ruling on a motion *in limine* for abuse of discretion." *United States v. Alvirez*, 831 F.3d 1115, 1120 (9th Cir. 2016). "However, we review *de novo* whether the ruling precludes the presentation of a defense." *Id.*

"[T]he Constitution guarantees criminal defendants a meaningful opportunity to present a complete defense," *Jones v. Davis*, 8 F.4th 1027, 1035 (9th Cir. 2021) (quoting *Crane v. Kentucky*, 476 U.S. 683, 690 (1986)), which includes "the right to put before a jury evidence that might influence the determination of

guilt," *id.* (quoting *Pennsylvania v. Ritchie*, 480 U.S. 39, 56 (1987)). "[A] defendant's right to present a complete defense is abridged by any restrictions on defense evidence that are 'arbitrary or disproportionate' and that infringe on the defendant's 'weighty interest.'" *Id.* at 1036 (quoting *Holmes v. South Carolina*, 547 U.S. 319, 324 (2006)).

Nonetheless, "[t]he accused does not have an unfettered right to offer testimony that is inadmissible under standard rules of evidence." *Id.* (cleaned up) (quoting *Taylor v. Illinois*, 484 U.S. 400, 410 (1988)). "A trial court therefore may, consistent with the Constitution, exclude defense evidence through the proper application of evidentiary rules that serve a valid purpose in a given case, including when proposed evidence is 'only marginally relevant or poses an undue risk of harassment, prejudice, or confusion of the issues.'" *Id.* (quoting *Holmes*, 547 U.S. at 326–27).

In a February 2019 email, Kvashuk informed the tax professional who prepared his 2018 tax return, Daniel Lusk, that he had purchased his house with "cash that my dad gave me." Lusk asked for documentation of the funding source, and Kvashuk sent him a tax report from his Coinbase account. Kvashuk explained: "[I]t's all that I have. My dad would use [Bitcoin] to send me cash for security reasons, I have pending asylum. He purchased [Bitcoin]-> send it to me-> I sell it here-> get cash."

Prior to trial, the prosecution moved to exclude references to Kvashuk's immigration status and asylum application, arguing it was irrelevant and unduly prejudicial under Federal Rules of Evidence 402 and 403. The district court granted this relief but allowed Kvashuk to testify "that he is from the Ukraine" and,

with adequate foundation, that he "transferred or received crypto currency" because he needed "to conceal the transfers from the Ukrainian government."

At trial, the prosecution elicited testimony from Lusk about the email exchange, a redacted copy of which was admitted into evidence. The redacted version omitted "I have pending asylum," leaving only "My dad would use [Bitcoin] to send me cash for security reasons." Later, the prosecutor reread the redacted email.

Kvashuk argues that the asylum ruling precluded him from presenting a complete defense because it "prevented [him] from making a full narrative regarding the legitimate reasons underlying his use of cryptocurrency." He claims that his "sole defense" to the prosecution's theory that he "used cryptocurrency to 'conceal the money trail from his crime'" was to show "that he did not intend to defraud Microsoft." Kvashuk wanted the jury to hear that he used Bitcoin "as an asylum seeker . . . to avoid detection by the Ukrainian government," because "Ukraine requires disclosure" of the receiver's location "for cross-border money remittances over a certain amount."

The district court's exclusion of evidence regarding Kvashuk's asylum status did not deny him a defense. The district court's restrictions on such evidence were narrowly tailored and carefully explained, not "arbitrary or disproportionate." *Jones*, 8 F.4th at 1036. While testifying about his asylum status may have strengthened his defense that he did not intend to defraud Microsoft, he was able to raise the defense without it.

Nor did the district court abuse its discretion in excluding the evidence. Although Kvashuk claims the jury equated his statement to Lusk that he used cryptocurrency "for security reasons" with "so I won't get caught by Microsoft," the jury also heard Kvashuk's statement to another tax professional that his father sent Bitcoin "because of his [father's] country restrictions." In addition, the district court allowed Kvashuk to testify "on [his] belief that he needed to conceal the transfer from the Ukrainian government," though he chose not to do so. The district court did not abuse its discretion in concluding, prior to trial, that any additional probative value in disclosing Kvashuk's immigration status "would be substantially outweighed by the danger of unfair prejudice" from the jury's knowledge that "Kvashuk could suffer immigration consequences if convicted of the charges." *See* Fed. R. Evid. 403.

At trial, Kvashuk understandably chose to abandon his story about his father transferring millions of dollars to him after the prosecution introduced evidence that his father earned only $1,150 per month in Ukraine. Instead, Kvashuk admitted to the jury that the Bitcoin came from sales of the stolen CSV and that he lied to the tax professionals about the Bitcoin's source because explaining the Paxful transactions would be more involved than simply saying the Bitcoin was a gift from his father. In light of Kvashuk's testimony, the district court did not abuse its discretion in ruling that the excluded evidence of Kvashuk's asylum status did not warrant a new trial. Any marginal probative value this evidence retained after he changed his story was substantially outweighed by the risk of juror confusion and prejudice to the prosecution. *See id.*

D. Motion to Dismiss Juror No. 12

Kvashuk lastly contends that the district court should have dismissed Juror No. 12 because the juror had experience with the UST. Our review of the district court's denial of a motion to dismiss a sitting juror depends on the ruling's basis. We review an actual bias determination for abuse of discretion; implied bias is a mixed question of law and fact that we review de novo. *United States v. Gonzalez*, 906 F.3d 784, 796 (9th Cir. 2018).

During voir dire, Juror No. 12 disclosed that he "was primarily employed as a Microsoft contractor between 2011 and 2018 on a variety of different projects" and that Microsoft was his current employer's "primary business partner." He professed having "a very wide and very shallow knowledge of almost any computer subject you can imagine." Nonetheless, he affirmed that he could "render an impartial verdict." Defense counsel asked no follow-up questions.

On the second day of the trial, after Wilcox testified about Kvashuk's role at the UST, Juror No. 12 sent a note to the court stating that he "work[ed] in close proximity" to "the people and teams being discussed" but did "not believe it to be a problem as [he] did not work directly with [them]." Upon further questioning, Juror No. 12 explained that he worked at Microsoft from April 2014 to August 2016, thus ending the same month Kvashuk started. According to Juror No. 12, the Universal Store "was just starting up when [he] was leaving," although he "was one of the early QA testers." However, the Universal Store had "advanced so far beyond what it was when [he] worked there, that it might as well be indistinguishable."

Juror No. 12 did not remember working on anything at Microsoft that had been discussed in the trial testimony and did not recognize any of the witnesses. He explained that he "worked on content ingestion," which involved the "people who were putting things for sale up on the storefront." It was "the exact opposite end" of what Kvashuk's team did "working on the user experience." Juror No. 12 reiterated that he could be fair and impartial.

Defense counsel moved to dismiss Juror No. 12. Counsel argued that had he known of the juror's "intimate knowledge of the Universal Store" during voir dire, he would have used one of his peremptory strikes on Juror No. 12 rather than one of the other prospective jurors. Defense counsel clarified, however, that he was not challenging Juror No. 12 based on his ability to be fair. The district court denied the request to remove Juror No. 12.

The district court, citing *Sanders v. Lamarque*, 357 F.3d 943 (9th Cir. 2004), evidently analyzed the request to remove Juror No. 12 as being for implied rather than actual bias. *See id.* at 948. Implied bias "is a legal doctrine under which bias will be conclusively presumed in certain circumstances even if the juror professes a sincere belief that she can be impartial." *Gonzalez*, 906 F.3d at 797. Bias will be presumed only in the extreme situation "where the relationship between a prospective juror and some aspect of the litigation is such that it is highly unlikely that the average person could remain impartial in his deliberations under the circumstances." *Id.* (quoting *Fields v. Brown*, 503 F.3d 755, 770 (9th Cir. 2007) (en banc)). Such a relationship exists, for example, when the juror has had a "personal experience that is similar or

identical to the fact pattern at issue in the trial," *id.* (quoting *United States v. Gonzalez*, 214 F.3d 1109, 1112 (9th Cir. 2000)), "'is aware of highly prejudicial information about the defendant,' which no ordinary person could be expected to put aside in reaching a verdict," *id.* (quoting *Gonzalez*, 214 F.3d at 1112), or "lies about material facts during *voir dire* in order to secure a spot on the jury," *id.*

Kvashuk argues that Juror No. 12 "must be dismissed because his extrinsic personal knowledge could cause him to make a decision based on information outside of the evidence presented at trial." But Juror No. 12 explained that his experiences at the UST in its early days were in no way similar to Kvashuk's experiences there a year or two later and that the Universal Store had changed considerably during that time. The UST had approximately 8,000 employees, and because Juror No. 12 and Kvashuk worked at different times on completely different aspects of the Universal Store, it is unlikely that their work overlapped. For example, there was no indication that Juror No. 12 had access to a TIP card since he did not work on the end user experience. Merely working for the same large organization as the defendant is an insufficient basis for implied bias.

We draw an analogy from *Frazier v. United States*, 335 U.S. 497 (1948). In that case, the defendant challenged two jurors because one juror and the other's spouse worked for the Treasury Department, which at the time contained the Bureau of Narcotics—the agency that had investigated the case. *Id.* at 512. In rejecting this challenge, the Court noted that the Treasury Department had 19,645 employees in the District of Columbia and that the two employees at

issue performed work unrelated to the Bureau of Narcotics. *Id.* at 499 n.2, 512. The Court held that this connection was "not so obvious a disqualification or so inherently prejudicial as a matter of law, in the absence of any challenge to [the jurors] before trial, as to require the court of its own motion or on [the defendant's] suggestion afterward to set the verdict aside and grant a new trial." *Id.* at 513.

Because Juror No. 12's "personal experience" on the UST was not "similar or identical to the fact pattern at issue in the trial," *Gonzalez*, 906 F.3d at 797, the district court properly denied the motion to remove him.

AFFIRMED.

JUDGMENT OF THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF WASHINGTON (NOVEMBER 9, 2020)

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

UNITED STATES OF AMERICA

v.

VOLODYMYR KVASHUK

Case No. 2:19CR00143JLR-001
USM Number: 49605-086

Before: Hon. James L. ROBART,
United States District Judge.

THE DEFENDANT:

☒ was found guilty on count(s) 1 through 18 after a plea of not guilty.

The defendant is adjudicated guilty of these offenses:

Title & Section	**Nature of Offense**	**Offense Ended**	**Count**
18 U.S.C. § 1029(a)(5)	Access Device Fraud	March 2018	1
18 U.S.C. §§ 1030(a)(4) and 1030(c)(3)(A)	Access to a Protected Computer In	March 2018	2

	Furtherance of Fraud		
18 U.S.C. § 1341	Mail Fraud	March 2018	3
18 U.S.C. § 1343	Wire Fraud	March 2018	4
18 U.S.C. § 1343	Wire Fraud	March 2018	5
18 U.S.C. § 1343	Wire Fraud	March 2018	6
18 U.S.C. § 1343	Wire Fraud	March 2018	7
18 U.S.C. § 1343	Wire Fraud	March 2018	8
26 U.S.C. § 7206(1)	Making And Subscribing To A False Tax Return	March 2018	9
26 U.S.C. § 7206(1)	Making And Subscribing To A False Tax Return	March 2018	10
18 U.S.C. § 1957	Money Laundering	March 2018	11
18 U.S.C. § 1957	Money Laundering	March 2018	12
18 U.S.C. § 1957	Money Laundering	March 2018	13

18 U.S.C. § 1957	Money Laundering	March 2018	14
18 U.S.C. § 1957	Money Laundering	March 2018	15
18 U.S.C. § 1957	Money Laundering	March 2018	16
18 U.S.C. § 1028A(c)	Aggravated Identity Theft	March 2018	17
18 U.S.C. § 1028A(c)	Aggravated Identity Theft	March 2018	18

The defendant is sentenced as provided in pages 2 through 8 of this judgment. The sentence is imposed pursuant to the Sentencing Reform Act of 1984.

It is ordered that the defendant must notify the United States attorney for this district within 30 days of any change of name, residence, or mailing address until all fines, restitution, costs, and special assessments imposed by this judgment are fully paid. If ordered to pay restitution, the defendant must notify the court and United States Attorney of material changes in economic circumstances.

/s/ Michael Dion
Assistant United States Attorney

November 9, 2020
Date of Imposition of Judgment

/s/ James L. Robart
The Honorable James L. Robart
United States District Judge

Date: November 9, 2020

IMPRISONMENT

The defendant is hereby committed to the custody of the United States Bureau of Prisons to be imprisoned for a total term of:

Counts 1-16: eighty four (84) months; Counts 17-18: an additional twenty four (24) months, to be served consecutively to the sentence for Counts 1-16; for a total sentence of one hundred and eight (108) months.

☒ The court makes the following recommendations to the Bureau of Prisons:

Placement at Sheridan Facility.

☒ The defendant is remanded to the custody of the United States Marshal.

SUPERVISED RELEASE

Upon release from imprisonment, you will be on supervised release for a term of:

Three (3) years

MANDATORY CONDITIONS

1. You must not commit another federal, state or local crime.
2. You must not unlawfully possess a controlled substance.
3. You must refrain from any unlawful use of a controlled substance. You must submit to one drug test within 15 days of release from imprisonment and at least two periodic drug tests thereafter, as determined by the court.

4. ☒ You must make restitution in accordance with 18 U.S.C. §§ 3663 and 3663A or any other statute authorizing a sentence of restitution. (*check if applicable*)

5. ☒ You must cooperate in the collection of DNA as directed by the probation officer. (*check if applicable*)

[. . .]

You must comply with the standard conditions that have been adopted by this court as well as with any additional conditions on the attached pages.

STANDARD CONDITIONS OF SUPERVISION

As part of your supervised release, you must comply with the following standard conditions of supervision. These conditions are imposed because they establish the basic expectations for your behavior while on supervision and identify the minimum tools needed by probation officers to keep informed, report to the court about, and bring about improvements in your conduct and condition.

1. You must report to the probation office in the federal judicial district where you are authorized to reside within 72 hours of your release from imprisonment, unless the probation officer instructs you to report to a different probation office or within a different time frame.

2. After initially reporting to the probation office, you will receive instructions from the court or the probation officer about how and when you must report to the probation officer, and you must report to the probation officer as instructed.

3. You must not knowingly leave the federal judicial district where you are authorized to reside without first getting permission from the court or the probation officer.

4. You must answer truthfully the questions asked by your probation officer.

5. You must live at a place approved by the probation officer. If you plan to change where you live or anything about your living arrangements (such as the people you live with), you must notify the probation officer at least 10 days before the change. If notifying the probation officer in advance is not possible due to unanticipated circumstances, you must notify the probation officer within 72 hours of becoming aware of a change or expected change.

6. You must allow the probation officer to visit you at any time at your home or elsewhere, and you must permit the probation officer to take any items prohibited by the conditions of your supervision that he or she observes in plain view.

7. You must work full time (at least 30 hours per week) at a lawful type of employment, unless the probation officer excuses you from doing so. If you do not have full-time employment you must try to find full-time employment, unless the probation officer excuses you from doing so. If you plan to change where you work or anything about your work (such as your position or your job responsibilities), you must notify the probation officer at least 10 days before the change. If notifying the probation officer at least 10 days in advance is not possible due to unanticipated circumstances, you

must notify the probation officer within 72 hours of becoming aware of a change or expected change.

8. You must not communicate or interact with someone you know is engaged in criminal activity. If you know someone has been convicted of a felony, you must not knowingly communicate or interact with that person without first getting the permission of the probation officer.

9. If you are arrested or questioned by a law enforcement officer, you must notify the probation officer within 72 hours.

10. You must not own, possess, or have access to a firearm, ammunition, destructive device, or dangerous weapon (*i.e.*, anything that was designed, or was modified for, the specific purpose of causing bodily injury or death to another person such as nunchakus or tasers).

11. You must not act or make any agreement with a law enforcement agency to act as a confidential human source or informant without first getting the permission of the court.

12. If the probation officer determines that you pose a risk to another person (including an organization), the probation officer may require you to notify the person about the risk and you must comply with that instruction. The probation officer may contact the person and confirm that you have notified the person about the risk.

13. You must follow the instructions of the probation officer related to the conditions of supervision.

SPECIAL CONDITIONS OF SUPERVISION

1. If deported, the defendant shall not reenter the United States without permission of the Secretary of the Department of Homeland Security. If granted permission to reenter, the defendant shall contact the nearest U.S. Probation Office within 72 hours of reentry.

2. Restitution in the amount of $8,344,586.31 is due immediately. Any unpaid amount is to be paid during the period of supervision in monthly installments of not less than 10% of his or her gross monthly household income. Interest on the restitution shall be waived.

3. The defendant shall provide the probation officer with access to any requested financial information including authorization to conduct credit checks and obtain copies of the defendant's federal income tax returns.

4. The defendant shall disclose all assets and liabilities to the probation office. The defendant shall not transfer, sell, give away, or otherwise convey any asset, without first consulting with the probation office.

5. If the defendant maintains interest in any business or enterprise, the defendant shall, upon request, surrender and/or make available, for review, any and all documents and records of said business or enterprise to the probation office.

6. The defendant shall maintain a single checking account in his or her name. The defendant shall deposit into this account all income, monetary gains, or other pecuniary proceeds, and make use of this account for payment of all personal expenses. This account, and

all other bank accounts, must be disclosed to the probation office.

7. The defendant shall participate as directed in the Moral Resonation Therapy program approved by the United States Probation and Pretrial Services Office. The defendant must contribute towards the cost of any programs, to the extent the defendant is financially able to do so, as determined by the U.S. Probation Officer.

8. The defendant shall submit his or her person, property, house, residence, storage unit, vehicle, papers, computers (as defined in 18 U.S.C. § 1030(e)(1)), other electronic communications or data storage devices or media, or office, to a search conducted by a United States probation officer, at a reasonable time and in a reasonable manner, based upon reasonable suspicion of contraband or evidence of a violation of a condition of supervision. Failure to submit to a search may be grounds for revocation. The defendant shall warn any other occupants that the premises may be subject to searches pursuant to this condition.

CRIMINAL MONETARY PENALTIES

The defendant must pay the total criminal monetary penalties under the schedule of payments on Sheet 6.

Assessment	$1800
Restitution	$8,344,586.31
Fine	Waived
AVAA Assessment*	N/A

* Amy, Vicky, and Andy Child Pornography Victim Assistance Act of 2018, Pub. L. No. 115-299.

JVTA Assessment** N/A

☒ The defendant must make restitution (including community restitution) to the following payees in the amount listed below.

Name of Payee	Microsoft Corporation
Total Loss***	$8,344,586.31
Restitution Ordered	$8,344,586.31
Priority or Percentage	100%

TOTALS	$8,344,586.31	$8,344,586.31

☒ The court determined that the defendant does not have the ability to pay interest and it is ordered that:

☒ the interest requirement is waived for the

☒ restitution

☒ The court finds the defendant is financially unable and is unlikely to become able to pay a fine and, accordingly, the imposition of a fine is waived.

SCHEDULE OF PAYMENTS

Having assessed the defendant's ability to pay, payment of the total criminal monetary penalties is due as follows:

☒ PAYMENT IS DUE IMMEDIATELY. Any unpaid amount shall be paid to Clerk's Office, United

---

** Justice for Victims of Trafficking Act of 2015, Pub. L. No. 114-22.

*** Findings for the total amount of losses are required under Chapters 109A, 110, 110A, and 113A of Title 18 for offenses committed on or after September 13, 1994, but before April 23, 1996.

States District Court, 700 Stewart Street, Seattle, WA 98101.

☒ During the period of imprisonment, no less than 25% of their inmate gross monthly income or $25.00 per quarter, whichever is greater, to be collected and disbursed in accordance with the Inmate Financial Responsibility Program.

☒ During the period of supervised release, in monthly installments amounting to not less than 10% of the defendant's gross monthly household income, to commence 30 days after release from imprisonment.

The payment schedule above is the minimum amount that the defendant is expected to pay towards the monetary penalties imposed by the Court. The defendant shall pay more than the amount established whenever possible. The defendant must notify the Court, the United States Probation Office, and the United States Attorney's Office of any material change in the defendant's financial circumstances that might affect the ability to pay restitution.

Unless the court has expressly ordered otherwise, if this judgment imposes imprisonment, payment of criminal monetary penalties is due during the period of imprisonment. All criminal monetary penalties, except those payments made through the Federal Bureau of Prisons' Inmate Financial Responsibility Program are made to the United States District Court, Western District of Washington. For restitution payments, the Clerk of the Court is to forward money received to the party(ies) designated to receive restitu-

tion specified on the Criminal Monetaries (Sheet 5) page.

The defendant shall receive credit for all payments previously made toward any criminal monetary penalties imposed.

Payments shall be applied in the following order: (1) assessment, (2) restitution principal, (3) restitution interest, (4) AVAA assessment, (5) fine principal, (6) fine interest, (7) community restitution, (8) JVTA Assessment, (9) penalties, and (10) costs, including cost of prosecution and court costs.

MINUTE ORDER ENTRY
DENYING MOTION TO SUPPRESS
(DECEMBER 16, 2019)

12/16/2019

75 MINUTE ENTRY for proceedings held before Judge James L. Robert–CRD: *Ashleigh Drecktrah*; AUSA: *Michael Dion*, *Siddharth Velamoor*; Def Cnsl: *Joshua Lowther*; Court Reporter: *Debbie Zurn;* MOTION HEARING as to Volodymyr Kvashuk held on 12/16/2019. For the reason stated on the record, the court riles as follows: United States' Motion in Limine to Exclude (Dkt. #54) is GRANTED in part and DENIED in part. Defendant's Motion to Dismiss Count 14 (Dkt. #55) is DENIED Defendant's Motion to Suppress Evidence (Dkt. #56) is DENIED. Defendant's Motion to Continue Trial (Dkt. #74) is GRANTED. A scheduling order will be entered setting the new trial date. Defendant remanded to custody. (AD) (Entered: 12/17/2019)

ORDER OF THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT DENYING PETITION FOR REHEARING (MAY 4, 2022)

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

VOLODYMYR KVASHUK,

Defendant-Appellant.

No. 20-30251

D.C. No. 2:19-cr-00143-JLR-1
Western District of Washington, Seattle

Before: PAEZ, M. SMITH, and
NGUYEN, Circuit Judges.

The panel has voted to deny the petition for panel rehearing. The panel has voted to deny the petition for rehearing en banc and Judge Paez has so recommended.

The full court has been advised of the petition for rehearing en banc and no judge has requested a vote on whether to rehear the matter en banc. Fed. R. App. P. 35.

The petition for panel rehearing and the petition for rehearing en banc are denied.

SEARCH WARRANT AFFIDAVIT
(JULY 11, 2019)

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON

In the Matter of the Search of
(Briefly describe the property to be searched or identify, the person by name and address)
A residence at 6409 Ripley Lane SE, and other locations, more fully described in Attachments A-1, A-2, and A-3,

Case No. MJ19-315

Before: Michelle L. PETERSON,
United States Magistrate Judge.

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 Attachments A-1, A-2, and A-3, incorporated herein by reference.

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

See Attachment B, incorporated herein by reference.

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;

The search is related to a violation of:

Code Section:
18 U.S.C. 1341, 1343, 1956 1957,
26 U.S.C. 7206(1)

Offense Description

Mail fraud, wire fraud, money laundering, filing a false tax return

The application is based on these facts:

✓ *See* Affidavit of SA Eric Hergert, continued on the attached sheet.

/s/ Eric Hergert
Applicant's signature

The foregoing affidavit was sworn to before me and signed in my presence,

/s/ Michelle L. Peterson
United States Magistrate Judge

Date: July 11, 2019
City and State: Seattle, Washington

AFFIDAVIT

STATE OF WASHINGTON
ss
COUNTY OF KING

I, Eric Hergert, being first duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with Internal Revenue Service, Criminal Investigation (IRS-CI), and have been so employed since September 2009. I am presently assigned to IRS-CI's Western Area Cyber Crime Unit in the Los Angeles Field Office. My duties and responsibilities include the investigation of possible criminal violations of the Internal Revenue laws (Title 26, United States Code), the Bank Secrecy Act (Title 31, United States Code), the Money Laundering Control Act of 1986 (Title 18, United States Code, Sections 1956 and 1957), and other related offenses.

2. I earned a Bachelor of Arts degree in accounting from the University of Washington, Tacoma, in 2002. I attended the Criminal Investigator Training Program and the IRS Special Agent Basic Training at the Federal Law Enforcement Training Center (FLETC) where I received detailed training in conducting financial investigations. The training included search and seizure, the Internal Revenue laws, and IRS procedures and policies in criminal investigations. I have also attended various cybercrime and virtual currency related trainings, including at FLETC and others.

3. Before being hired by IRS-CI, I was employed as a Revenue Agent for the IRS for approximately five years, performing civil examinations of small busi-

nesses and self-employed individuals. As a Revenue Agent, I received approximately 16 weeks of specialized training in personal, partnership, and corporate income tax, as specified in the Internal Revenue Code.

4. I have conducted and assisted in numerous investigations involving financial crimes. I have led and participated in the execution of search warrants and have interviewed witnesses and defendants who were involved in, or had knowledge of, violations of the Internal Revenue Code, the Bank Secrecy Act, and the Money Laundering Control Act. In the course of my employment with IRS-CI, I have conducted and have been involved in investigations of alleged criminal violations, which have included tax evasion (26 U.S.C. § 7201), filing a false tax return (26 U.S.C. § 7206(1)), aiding or assisting in the preparation of false tax returns (26 U.S.C. § 7206(2)), conspiring to defraud the United States (18 U.S.C. § 371), wire and mail fraud (18 U.S.C. §§ 1343, 1341), aggravated identity theft (18 U.S.C. § 1028A), and money laundering (18 U.S.C. §§ 1956, 1957), among others.

5. I have led and participated in the execution of federal search warrants and the consensual searches of records relating to the concealment of assets and proceeds derived from fraud. These records included, but were not limited to, email accounts, instant messages, personal telephone books, photographs, bank records, escrow records, credit card records, tax returns, business books and records, and computer hardware and software.

6. I also have specialized training in cryptocurrencies, with a focus on Bitcoin and Ethereum. This has included training into how publically viewable "blockchains" record cryptocurrency transactions, how

to trace funds through these transactions, attribution techniques used to identify individuals responsible for conducting the transactions, and methods used by individuals to obfuscate the source of, or their control of, cryptocurrencies. I have used these techniques in 'prior and ongoing investigations. Additionally, I have conducted cryptocurrency training for others, both internal to the IRS, as well as for external third parties.

7. 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 following locations, more fully described in Attachments A-1, A-2, and A-3 to this Affidavit, for the property and items described in Attachment B to this Affidavit, as well as any digital devices or other electronic storage media located therein. Attachments A-1, A-2, A-3, and Attachment B are attached hereto and incorporated herein by this reference.

8. The premises located at 6409 Ripley Lane Southeast, Renton, Washington, hereinafter "SUBJECT LOCATION," further described in Attachment A-1.

9. The Tesla vehicle with VIN 5YJSA1E40J F249750, hereinafter "SUBJECT VEHICLE," further described in Attachment A-2.

10. The person of VOLODYMYR KVASHUK, hereinafter "KVASHUK." KVASHUK is a twenty-five (25) year-old male, with dark brown hair, brown eyes, a height of six feet and one inch, and weighing 175 pounds, per the Washington State Department of Licensing. KVASHUK is further described in Attachment A-3.

11. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained

from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

12. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not detail each and every fact and circumstance I or others have learned during the course of this investigation. Furthermore, the investigation is ongoing, including the gathering and analysis of records. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits and instrumentalities of Mail Fraud, in violation of Title 18, United States Code, Section 1341, Wire Fraud, in violation of Title 18, United States Code, Section 1343, Money Laundering, in violation of Title 18, United States Code, Sections 1956(a)(1) and 1957, and Filing a False Tax Return, in violation of Title 26, United States Code 7206(1), will be found at the SUBJECT LOCATION, in the SUBJECT VEHICLE, and on KVASHUK's person.

SUMMARY OF THE FRAUDULENT SCHEME

13. The target of this investigation is VOLODYMYR KVASHUK. The investigation has shown that KVASHUK devised and executed a scheme to defraud Microsoft Corporation ("Microsoft"). KVASHUK worked for Microsoft and was assigned to test the company's online retail sales platform. In that role, KVASHUK was supposed to make simulated purchases

of Microsoft products from the company's online store. The testing system was designed to ensure that no physical products would be shipped. KVASHUK, however, used test accounts to purchase massive amounts of "currency stored value," or "CSV," such as digital gift cards. The testing program was not supposed to involve purchases of CSV, and no mechanisms were in place to prevent the delivery of valuable CSV to the tester. The investigation has shown that KVASHUK, in his role as a tester, purchased millions of dollars of CSV, which he then resold on the Internet. KVASHUK used the proceeds of the fraud to purchase, among other things, a $160,000 Tesla car and a $1.6 million home in Renton.

SUMMARY OF THE INVESTIGATION

14. As part of this investigation, I have obtained records from numerous sources, met with counsel for Microsoft, and interviewed Microsoft employees who investigated the CSV theft.

Microsoft's Program to Test Online Retail Sales

15. Microsoft has given me a copy of VOLODYMYR KVASHUK's resume,' which shows that he is a Seattle-based software engineer. According to information provided by Microsoft, KVASHUK was an employee of a Microsoft vendor. As part of his employment with the vendor, KVASHUK worked on matters for Microsoft from August 26, 2016, until October 1, 2017. During that time, KVASHUK worked out of Microsoft's office and had access to the company's computer network. On December 1, 2017, Microsoft hired KVASHUK as a full-time employee with an annual salary of approx-

imately $116,000. KVASHUK worked for Microsoft until June 22, 2018.

16. Microsoft sells various products to the general public over the Internet via its online store. To make purchases from the Microsoft store, a customer must establish a Microsoft store account that is linked to an email address and to one or more payment devices (such as a credit card). As both an employee of an outside vendor, and as a Microsoft employee, KVASHUK was a member of Microsoft's Universal Store Team ("UST"), which supports the company's online retail platform by (among other things) managing a program that tests the online sales system.

17. The testing program involves creating test Microsoft store accounts that are linked to test email accounts created specifically for the purpose of the testing program. A tester creates a test email account by using a naming convention for the account: the name begins with "mstest," followed by an underscore and the user name of the tester. The tester then requests that the UST team "whitelist" the account, meaning that purchases made from the account will automatically bypass Microsoft's security and risk protocols, which monitor online purchases in order to detect possible fraud. The test accounts are linked to artificial payment devices ("Test in Production" or "TIP" cards)—in effect, phony credit cards—that allow the tester to simulate a purchase without generating an actual charge. Once the whitelisted account is created, the tester uses that account to attempt to make online product purchases from Microsoft, just as an ordinary consumer would. Although each test account was created for a particular tester, the login and password information for the test accounts was

stored in an electronic document that was accessible to multiple testers. Microsoft investigators told me that, in practice, testers sometimes used test accounts set up for other testers.

18. According to Microsoft, the testing program was designed to test the company's online sales of physical goods only. When a tester used a whitelisted account to purchase physical goods, the system ensured that no goods were actually delivered.

19. According to Microsoft, the testing program was not designed for simulated purchases of electronic currency stored value ("CSV"), such as digital gift cards. Testers were not authorized to use test accounts to make test purchases of CSV. Because Microsoft did not expect testers to purchase CSV, the system had no safeguards to prevent the delivery of actual, usable CSV to a tester who made a purchase from a whitelisted account. Accordingly, if a tester did purchase CSV, the system would generate a valid and usable product "key" that could be "redeemed," meaning that the value of the digital currency would be added to an electronic "wallet" linked to a customer account. Once redeemed, the CSV could be used to buy both physical and digital products from the Microsoft store.

The Theft of $10 Million in Microsoft's Digital Currency

20. According to information provided by Microsoft, in February of 2018, Microsoft's UST Fraud Investigation Strike Team ("FIST") noticed a suspicious increase in the use of CSV to buy subscriptions to Microsoft's Xbox live gaming system from Microsoft's online store. FIST investigated and discovered that the suspicious CSV had originally been purchased from

Microsoft through two whitelisted test accounts associated with the email accounts mstest_avestu@outlook .com and mstest_sfwe2eauto@outlook.com (the "avestu" and "sfwe2eauto" test accounts). The CSV was then resold on the secondary market, at a steep discount, via at least two online reseller websites, g2a.com and nokeys.com. Customers who purchased the CSV on the secondary market then redeemed the CSV at Microsoft's online store for Xbox live subscriptions.

21. The websites g2a.com and nokeys.com are located at IP addresses 88.198.39.152 and 67.229.64.252, respectively. According to open source research, the servers hosting these websites are located in Germany and California, respectively. All transmissions of CSV information to be sold through these websites are communication by wire through interstate or foreign commerce if those transmissions originate in Washington state.

22. The avestu and sfwe2eauto test accounts were not established by KVASHUK, but rather by other Microsoft employees. However, the username and passwords for those and other test accounts were stored on Microsoft's network, giving KVASHUK and many other Microsoft employees access to them. FIST discovered that the avestu and swfe2eauto test accounts were used to buy a large amount of CSV between November 2017 and March 2018. The avestu and swfe2eauto accounts were blocked by Microsoft on or about March 15, 2018. FIST later discovered that a third test account linked to mstest_ zabeerj2@ outlook.com (the "zabeerj2" test account) was also responsible for a suspicious spike in CSV purchases, conducting approximately 166 purchases of CSV

between March 22 and March 23, 2018. This account was blocked on or about March 23, 2019

23. The three suspicious test accounts were used to purchase roughly $10.1 million in CSV from Microsoft. Microsoft was able to "blacklist" roughly $1.8 million in CSV to prevent it from being redeemed, resulting in a total loss to Microsoft of approximately $8.3 million.

CSV REDEMPTIONS BY ACQUISITION ACCOUNT

Account	2017	2018	Total
Mstest_avestu	$357,595.00	$1,298,010.00	$1,655,605.00
Mstest_swfe2eauto	$601,261.27	$5,444,340.04	$6,045,601.31
Mstest_zabeerj2	$0.00	$643,380.00	$643,380.00
Total	**$958,856.27**	**$7,385,730.04**	**$8,344,586.31**

Account	**2017**	**2018**
Mstest_avestu	$357,595.00	$1,298,010.00
	Total	$1,655,605.00
Account	**2017**	**2018**
Mstest_swfe2eauto	$601,261.27	$5,444,340.04
	Total	$6,045,601.31
Account	**2017**	**2018**
Mstest_zabeerj2	$0.00	$643,380.00
	Total	$643,380.00
Total	**$958,856.27**	**$7,385,730.04**
	Total	**$8,344,586.31**

24. Microsoft interviewed the employees who created the three suspicious test accounts and found no evidence that they were involved in the fraudulent CSV purchases.

Evidence of Kvashuk's Involvement in the Theft

25. A variety of evidence shows that KVASHUK was involved in the CSV theft from Microsoft.

Kvashuk's Use of His Own Test Account for Theft

26. As an initial matter, KVASHUK has admitted to Microsoft investigators that he used the Microsoft store test account that he created—linked to mstest_v-vokvas@outlook.com (the "vokvas" test account")—to make unauthorized purchases. Microsoft records show that the vokvas test account made purchases (typically of CSV) on April 28, July 10, September 29, October 4, October 7, October 11, and October 22 of 2017. The amount of CSV obtained through the vokvas account totaled approximately $12,304.99, of which approximately $4,464.99 was redeemed.[1]

27. On October 7, 2017, the vokvas test account was used to purchase an electronic "token" for a subscription to Microsoft Office for $164.99. That token was redeemed by a Microsoft store account linked to the email address admin@searchdom.io. Microsoft records show that the name on the Microsoft online store account for "searchdom" is "Volo kvashuk," and the address is an apartment complex, 5035 15th Avenue, Unit 101, in Seattle (the "15th Avenue" apartment). A copy of KVASHUK 's resume (provided by Microsoft) lists him as the co-founder and Chief Technology Officer of "SearchDom." Washington Secretary of

[1] Approximately $100 of the redeemed CSV appears to have been in Canadian currency. It was not possible to determine from the records available how much of the $12,3043.99 in CSV obtained through the vokvas account was in a foreign currency.

State records list KVASHUK as a "governor" for Searchdom, Inc. Also listed as a "governor" in Secretary of State records is "L.W." Additionally, L.W. is the registrant contact for the domain name searchdom.io. According to records obtained from Namecheap, the domain name was registered in January 21, 2017.

28. According to Microsoft records, KVASHUK's vokvas test account was used to purchase approximately $10,164.99 in CSV in October 2017.

29. On October 22 and 24, 2017, approximately $2,500 in CSV obtained by the vokvas test account was redeemed to Microsoft store accounts linked to the email addresses pikimajado@tinoza.org (the "pikimajado" account) and xidijenizo@axsup.net (the "xidijenizo" account). Subscriber information has not been obtained for these email addresses. Based on my open source research, it appears these email addresses may be associated with temporary email services. These services often do not log subscriber information, and only keep the email account active for a few minutes.

30. On October 22 and 24, 2017, the redeemed funds in the pikimaj ado and xidijenizo accounts were used to order three GeForce GTX 1070 video or "graphics" cards with a total cost of approximately $2,024.58 from Microsoft's online store.[2] Microsoft's records show that the name and address associated with the Microsoft online store accounts linked to the pikimajado and xidijenizo email accounts is "Grigor shikor" at the same 15th Avenue apartment complex

[2] Microsoft records show attempts to access the vokvas test account from IP addresses located in Russia and Japan on October 22, 2017. These may have been attempts by KVASHUK to disguise his IP address, although that has not been confirmed.

that KVASHUK lived at, but at Unit 309 (instead of KVASHUK's unit, 101). Microsoft provided the FedEx tracking numbers for the shipment of these cards. By entering the tracking numbers into FedEx's website, I was able to determine that the video cards were shipped from Ontario, California to Seattle, Washington on or about October 22nd and 24th of 2017. Additionally, FedEx's website indicated that at least one of the video cards was delivered to the recipient address.

31. From my training and experience, I know that FedEx is a "private or commercial interstate carrier" as that term is used in Title 18, United States Code, Section 1341.

32. Public records searches did not identify anyone by the name of "Grigor Shikor" in Washington. However, a Grigoriy Kvashuk was identified as living in Oregon. As part of my investigation, I obtained phone records for 951-397-8122, which is listed as KVASHUK's phone on his resume. The subscriber name on that account is "Grigory Kvashuk." Additionally, the Washington Department of Licensing lists KVASHUK and Grigoriy Kvashuk as registered owners of a Honda Insight.

33. According to Microsoft records, approximately $600 of the CSV purchased by the vokvas account was redeemed to a Microsoft store account linked to the email address safirion@outlook.com (the "safirion" account). The registered name associated with the safirion@outlook.com email account is "volo kv". The current address is on 7th Avenue in Seattle, and the former address was KVASHUK's apartment at the 15th Avenue complex.

34. Microsoft investigators interviewed KVASHUK on May 10 and May 18 of 2018. Although no law enforcement officer was at those interviews, I have listened to recordings of the interviews. The interviews were not completely recorded because of a technical problem, but I have also read summaries of the interviews and spoken with Microsoft investigator Andy Cookson, who was present at both interviews.

35. The interviewers asked KVASHUK about the purchases made with the vokvas test account. KVASHUK admitted that he had created the vokvas account. He also admitted to making some unauthorized purchases from the account. KVASHUK suggested that there was a lack of guidance from his superiors about what could and could not be purchased via a test account, and claimed to have only been told that test accounts should not be used to purchase subscriptions.[3] KVASHUK claimed that he believed it was permissible to use test accounts to buy CSV because it was not "real" money.

36. KVASHUK admitted to Microsoft investigators that he used his test account to purchase CSV. He admitted that the "safirion" account was his personal account, and that he used stolen CSV to buy movies from the Microsoft store. KVASHUK admitted that he had tried to buy a video card, but claimed that it had never arrived.

37. The investigators asked KVASHUK about the video cards purchased (using CSV obtained by the

---

[3] Microsoft investigators have told me that the testers may not have been specifically told that purchasing CSV was prohibited, as the possibility that testers would purchase CSV was simply not contemplated.

vokvas test account) in the name of "Grigor Shikor" at Unit 309 of the 15th Avenue complex. KVASHUK denied purchasing those cards. When asked if he knew "Grigor Shikor," KVASHUK initially said, "it's complicated," but then denied knowing him.[4] KVASHUK admitted that he lived at the 15th Avenue complex, but denied receiving the cards.

38. With respect to the Office subscription purchased by the searchdom account (using a token obtained by the vokvas test account), KVASHUK said that he and another person were business partners in SearchDom. KVASHUK said that he did not remember this event and suggested that he might have made a mistake.

39. According to Microsoft records, prior to November 22, 2017, all of the CSV acquired through the vokvas account was redeemed to Microsoft online store accounts associated with the email addresses admin@searchdom .io, xidijenizo@axsup.net, or pikimajado@tinzoa.org.

40. According to records obtained from Google, on November 22, 2017, at approximately 12:17 PM, KVASHUK conducted an internet search for "cash in xbox gift." Then KVASHUK immediately visited the website, gameflip.com. Gameflip.com advertises that it allows users to list Xbox Live gift cards for sale on its site. After a gift card is purchased by a customer, Gameflip.com deposits the proceeds into the seller's "gameflip wallet." The seller can then withdraw the proceeds "any time into your PayPal, bank account, or Bitcoin."

---

[4] This part of the interview was not recorded.

41. Subsequently, on November 22, 2017, at approximately 7:48 PM, $50 Canadian of CSV acquired through the vokvas account was redeemed to an unknown individual's Microsoft store account associated with the email address sunmoon94@hotmail.com Over the next few days, approximately 12 more redemptions of CSV acquired by the vokvas account (totaling approximately $1,150 ($50 of which was Canadian)) were made to Microsoft store accounts associated with email addresses with no known connection to KVASHUK. Based on this information, it appears he began selling the CSV through third party websites on or about November 22, 2017.

Evidence Linking KVASHUK to CSV Thefts Through Other Test Accounts.

42. The vast majority of the $10 million in stolen CSV was obtained through the avestu, sfwe2eauto, and zabeerj2 test accounts. As noted, although these accounts were created by other testers, KVASHUK would have had access to the login information necessary to access these accounts. Furthermore, Microsoft investigators told me that—by using test accounts set up for other testers, rather than this own test account—KVASHUK made it more difficult for Microsoft to identify him as a suspect in the thefts.[5] Based on information provided by Microsoft, it appears that these accounts were used to make unauthorized CSV purchases from approximately November 26, 2017,

---

[5] As previously noted, Microsoft investigators also told me that the test accounts were sometimes shared among testers who were using the accounts for legitimate testing.

through March 23, 2018.[6] As best as can be determined from the available information, it appears that CSV was resold (most likely at a steep discount) through online resellers to customers who used the CSV to make purchases from Microsoft's online store.

43. Although KVASHUK admitted to only making very limited purchases of CSV from his test account, the investigation has shown probable cause to believe that KVASHUK used the avestu, sfwe2eauto, and zabeerj2 accounts to make unauthorized CSV purchases. Some of the evidence comes in the form of Internet Protocol ("IP") address data. An IP address is a numerical label assigned to each device that is connected to a computer network that accesses the Internet. In general, Microsoft's online sales platform records the IP addresses used to access the company's website. However, because the test accounts bypassed several safeguards, IP addresses were only captured on approximately 489 of 1,554 transactions.

44. Microsoft records show that between December 29, 2017, and March 23, 2018, at least $2.4 million of CSV was purchased using the avestu, sfwe2eauto, and zabeerj2 accounts in over 400 transactions from devices using at least 34 different IP addresses beginning with 173.244.44, including IP addresses 173.244.44.19 (February 2018 and March 2018), 173.244.44.37 (December 2017 and March 2018), 173.244.44.58 (February 2018 and March 2018), and 173.244.44.89 (January 2018, February 2018, and March 2018). Microsoft investigators initially told me

---

[6] KVASHUK was not employed at Microsoft for the early part of this time period, but could have used any Internet-enabled device to access and log into the test accounts.

that they believed that the IP addresses beginning in 173 were publicly-available IP address (such as one might find at a coffee shop with WiFi) because other Microsoft employees had logged in via these addresses. As set forth below, however, my investigation suggests that "173" IP addresses are not publicly available.

45. The investigation has shown that KVASHUK used a 173.244.44.* IP address to access a Microsoft store account linked to his personal email address, kvashuk.volodymyr@gmail.com (the "kvashuk" account)[7] at least nine times between December 2 and December 19 of 2017, including IP addresses 173.244.44.19, 173.244.44.37, and 173.244.44.58. He also logged into his Coinbase cryptocurrency account using IP address 173.244.44.89 on December 2, 2017. However, no incidents have been identified where KVASHUK used a 173.244.44.* IP address and a test account used the same IP address on the same day to purchase CSV.

46. Records obtained through the course of the investigation indicate that IP addresses 173.244.44.19, 173.244.44.37, 173.244.44.58, and 173.244.44.89 are assigned to the company London Trust Media, Inc. This company operates a virtual private network[8]

---

[7] The kvashuk.volodymyr@gmail.com account is listed as KVASHUK's personal account on his resume.

[8] A virtual private network (VPN) is programming that creates a safe and encrypted connection over a less secure network, such as the public internet. A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols. In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. Often times, a VPN will also provide a proxy server service. With this service, a user's true IP

(VPN) service that specializes in anonymity online under the name Private Internet Access through the website www.privateinternetacess.com. The use of a VPN can effectively conceal the true IP addresses that somebody is using to connect to the Internet. While I am continuing to investigate the 173.244.44.* IP addresses, I believe that all of the 173.244.44.* IP addresses associated to this investigation are controlled by London Trust Media, Inc. Microsoft records show that Microsoft employees other than KVASHUK have logged in via the 173.244.44.* IP addresses. Based on my training and experience, this does not suggest that the IP addresses are publicly available, but rather that other Microsoft employees have also used the London Trust VPN service.

47. Internet activity associated with the kvashuk.volodymyr@gmail.com account obtained from Google via a search warrant shows that KVASHUK conducted searches for terms related to, or visited websites for, Private Internet Access (or "PIA") at least once on November 27, 2017, and at least six times on December 17, 2017. The internet searches include the terms "pia hide tor traffic," "pia," "pia port forwarding," and "pia virus." Google records show he visited a Private Internet Access helpdesk article shortly after conducting these searches titled "Can I use TOR[9] with the Private

---

address is masked when accessing resources on the internet, such as websites. The internet resource would only be able to see the IP address of the proxy server.

9 In this context, TOR appears to be an acronym for "The Onion Router." TOR is an open-source software program that allows users to disguise their IP address through encryption and by bouncing their internet traffic through multiple other computers on the interne while operating compatible software.

Internet Access service." These searches suggest that, during the same time that the fraud scheme was ramping up, KVASHUK was researching ways to conceal his identity on the Internet.

48. According to records obtained from Microsoft, the first date a 173.244.44.* IP address was used to obtain CSV as part of this scheme was on December 29, 2017, when a CSV "purchase" was made through the avestu account. IP addresses in the 173.244.44.* range were used several times to obtain CSV through the avestu, sfwe2eauto, and zabeerj2 accounts through March 23, 2018.

49. Based on my training and experience, KVASHUK may have believed that by using a VPN service specializing in online anonymity to commit the fraud, he could disguise his involvement in the crimes. Specifically, according to the Private Internet Access website, their VPN service provides "IP Cloaking" by masking a user's IP address with one of their anonymous IP addresses. Based on KVASHUK's experience as a software developer, and his experience working with Microsoft on their online store, I believe he would know that the Microsoft online store records the IP address of the users conducting transactions, and that a VPN service would mask his true IP address, thereby disguising his involvement.

50. Another IP address, 4.35.246.19, was also used to access the avestu and sfwe2eauto test accounts at least 24 times for purchases of over $131,000 in CSV in connection with the fraud. The IP address was also used to access three Microsoft store accounts linked to KVASHUK. It was used at least 54 times between October 24, 2017 and November 24, 2017 to access the pikimajdo and xidijenizo accounts (the

accounts used to order the graphics cards delivered to "Grigory Shikor" at KVASHUK's apartment complex) and used at least 21 times on November 24, 2017 to access the vokvas test account (the test account created by KVASHUK). This IP address is registered to Level 3 Communications. By the time this IP address was provided to investigators, subscriber records for the dates and times in question were outside of Level 3 Communications' retention period.

51. A third IP address, 50.243.108.211, was used five times on December 12, 2017, to purchase approximately $39,500 of CSV using the sfwe2eauto test account. It was also used to access the vokvas account on June 5, 2017 and October 22, 2017, and the xidijenizo account on October 22, 2017. The same IP address had also been used on February 20, 2017 by KVASHUK when opening an account with the cryptocurrency exchange Coinbase. As discussed below, KVASHUK deposited at least some of the proceeds of the fraud into this Coinbase account. Level 3 Communications also provides end user service for this IP address. By the time this IP address was provided to investigators, subscriber records for the dates and times in question were outside of Level 3 Communications' retention period.

52. The fact that all of the above IP addresses are linked to both KVASHUK and the test accounts used to commit the fraud strongly suggests KVASHUK's involvement in the crime.

53. KVASHUK is also linked to the avestu and sfwe2eauto accounts through a technology known as "Fuzzy Device" identification. When a person uses a particular device to access Microsoft's online store, that device leaves a digital trail known as a "Fuzzy

Device" identifier. According to Microsoft, although it is theoretically possible for two devices to have the same Fuzzy Device ID, it is very unlikely. As a result, if multiple logins are made from the same Fuzzy Device ID, there is a strong inference that the same device (a particular computer, cell phone, etc.) was used to make all of those logins.

54. Between October 22, 2017, and November 26, 2017, Microsoft's records show the same Fuzzy Device ID for logins to accounts known or believed to be associated with KVASHUK (the vokvas, xidijenizo, and pikimajado accounts) as well as at least some logins to the accounts by which most of the CSV was stolen (avestu and sfwe2eauto). Similarly, Microsoft records show that the user who logged into all of those accounts was, on at least some occasions, running the same version of the Linux operating system and the same outdated version of the Mozilla Firefox browser—further evidence that a single device logged into all of those accounts.

55. The fuzzy device ID bb92c484-876b-4d87-adca-943b90a2d98e (the "98e" ID) was the only fuzzy device ID used to make purchases on the Microsoft online store by the accounts associated with the email addresses pikimajado@tinzoa.org and xidijenizo@axsup.net. The 98e ID was also used to make purchases on the Microsoft online store by the vokvas, avestu, and swfe2eauto accounts. According to Microsoft, no other Microsoft store accounts were associated with the 98e ID.

56. Based on my training and experience, I know that the term "Device ID" is a generic industry term for an identifier for an electronic device. Some devices have a unique identifier specifically labeled as a "Device

ID" by a hardware manufacturer. When one hardware manufacturer, website, government agency, or any other company refers to the identification of, collection of, or use of a "Device ID," they are generally talking about a different identifier or mechanism for generating a Device ID that is unique to that manufacturer or other entity. Device IDs are generally used to identify multiple transactions conducted by the same device.

57. I also know that Device IDs are often created by collecting a very large collection of not-so-unique browser and system components that a web-browser allows a website to view/collect, such as operating system, web-browser, screen resolution, and many other settings. If any of the settings used to calculate the Device ID change, the Device ID will change. An individual with knowledge of Device IDs could disguise the fact that they are conducting multiple transactions from the same device by changing some of these settings. Additionally, Device IDs would change if the individual used more than one device, or used virtual machines[10] to simulate the use of more than one device.

58. In total, Microsoft captured Fuzzy Device ID information on approximately 223 of the 1,554 purchases of CSV using the avestu, sfwe2eauto, and zabeerj2

---

[10] A virtual machine is simulated computer that runs its own operating system that runs like an application on another computer. The end user has a similar experience on a virtual machine as they would have if the operating system were installed on its own device. Several virtual machines can be installed on a single computer, and can be created in a short period of time. The use of a virtual machine could conceal the Device ID of the underlying device.

accounts.[11] Over the course of the scheme, a total of 14 different Fuzzy Device IDs were captured on these 223 transactions. Most of the Fuzzy Device IDs were only used to purchase the CSV for one day. This could be indicative of using multiple devices, or the use of virtual machines. The first Fuzzy Device ID listed on the chart below–the 98e address–was used to access the vokvas, xidijenizo, and pikimajado accounts between October 22 and 24, 2017, and was also used to access the avestu and sfwe2eauto test accounts to make CSV purchases on November 26, 2017. This strongly suggests that the same device was used to access both accounts known to be linked to KVASHUK as well as the test accounts used to commit the fraud.

Device ID	Identified Purchase Transactions	Date Range
bb92c484-876b-4d87-adca-943b90a2d98e	6	11/26/2017
58b04a06-d52c-481b-9050-34d1f5c64aab	20	12/2/2017–12/13/2017
3ab2d39-29f9-4332-bc96-3121a57d99cd	1	12/3/2017
c2313cdc-a005-421b-9fa9-159d2adbdf53	3	12/7/2017

[11] Fuzzy Device ID information was only captured for transactions conducted through the avestu and sfwe2eauto accounts.

aa29eee2-3f6d-45b4-9c01-cfa320b962b1	11	12/9/2017–12/12/2017
455010cd-e513-44c1-8fc0-f4495b0d7453	6	12/10/2017
6d2a6011-99b5-48be-b00c-130450b26272	12	12/14/2017
d117e690-0627-4624-912f-3a636457bf6d	19	12/15/2017
ec76885c-6718-4857-8cd9-8ea3f11ed30e	12	12/16/2017
84925e6b-035f-4138-9b41-b2dbbb13efce	10	12/17/2017
3b0d8c07-3656-4c4c-b938-8441c8c43716	17	12/19/2017–12/20/2017
21c35123-ccef-474f-ade4-8fd96984975d	79	12/22/2017–1/4/2018
486e5a23-b428-478c-99ed-7c25c8d76b25	25	1/12/2018
0424b94c-9e86-4abd-a9f4-bfce92f962a1	2	1/20/2018

Internet activity associated with the kvashuk.volodymyr @gmail.com account obtained from Google via a search warrant shows that KV ASHUK searched for terms related to, or visited websites for or related to, "VM" or "virtualbox" (a virtual machine software) at least twenty times between November 7, 2017, and November 25, 2017.

Evidence of Unexplained Wealth

59. Financial records show that KVASHUK had a large amount of unexplained income during the period of the CSV thefts. According to his tax returns for 2016 and 2017, KVASHUK only had total income of $35,260 and $114,103, respectively. According to Microsoft, for the portion of time KVASHUK was a direct employee (December 2017 to June 2018), his annual salary was $116,000.

60. I have reviewed records for a checking account that KVASHUK had at Wells Fargo bank, ending in -5789. The earliest daily balance shown on the records was $429.56 on July 29, 2016. The balance on the account remained under $20,000 until late November of 2017, when large amounts of money from a cryptocurrency account in KVASHUK's name at Coinbase .com, began to flow into the -5789 account. On November 30, 2017, over $14,000 was transferred to the -5789 account from Coinbase.com.[12] On December 11, 2017, over $6,600 was transferred from Coinbase.com to the -5789 account. On December 21, 2017, there was a

[12] Of the $14,876.98 transferred, $5,024.01 was proceeds from the sale of Ethereum cryptocurrency. This cryptocurrency had been obtained in June 2017, and is not believed to be proceeds from the wire fraud scheme.

transfer of over $29,000 from Coinbase.com to the -5789 account.

61. The suspicious transfers escalated dramatically in early 2018. For example, on January 30th, February 2nd, and February 6th of 2018, there were transfers from Coinbase of over $98,000, $177,000 and $134,000, respectively. On a single day March 2, 2018– over $500,000 was transferred from Coinbase to the -5789 account. Over $1.4 million was transferred in total in March 2018, followed by over $935,000 in April.

62. All told, over $2.8 million was transferred from Coinbase to the -5789 11 account between November 2017 and May 2018. The approximate timeframe of the vast majority of the fraud was November 2017 through March 2018. Given these timeframes, and based on my training and experience, it appears that KV ASHUK had converted the proceeds of the fraud into cryptocurrency (or received the proceeds as cryptocurrency), and then gradually converted the cryptocurrency in fiat currency and transferred the proceeds to his Wells Fargo account.

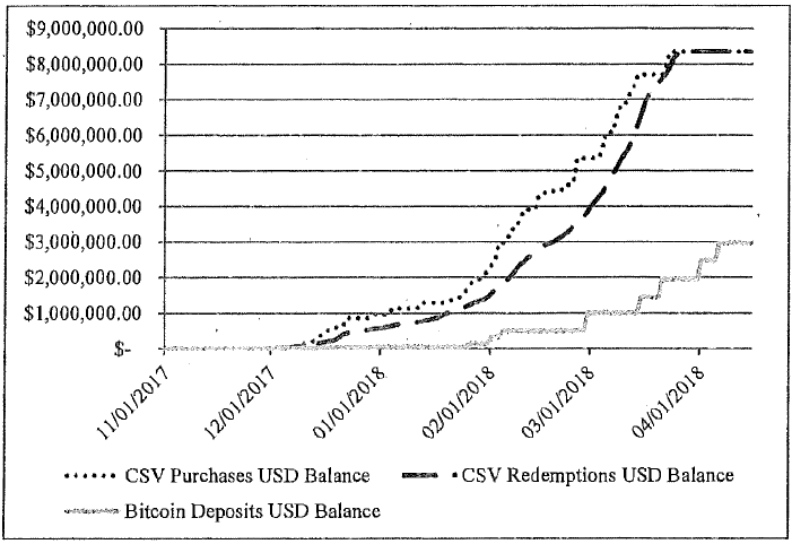
63. Furthermore, in order to determine the source of the cryptocurrency "bitcoin" in the Coinbase account, I have examined the bitcoin blockchain, a public ledger of bitcoin transactions. I determined that the vast majority of the bitcoin deposited into the Coinbase account originated from chipniixer.com. Chipmixer.com is a bitcoin "mixing" service which appears to be located in Germany. A bitcoin mixing service mixes potentially identifiable bitcoin with others, with the intent to obscure and conceal the original source of the bitcoin. Based on my training and experience, the use of chipmixer.com is further evidence of an attempt to conceal proceeds of the fraud.

64. In addition to the bitcoin sourced from chipmixer.com, I was able to trace a deposit of 1.5 bitcoin into KVASHUK's Coinbase account on November 29, 2017 from Paxful.com. Paxful.com is a peer-to-peer cryptocurrency trading site. This site allows users to purchase bitcoin with gift cards, including Xbox gift cards. Internet activity associated with the kvashuk .volodymyr@gmail.com account obtained from Google via a search warrant showed KVASHUK searched for terms related to, or visited websites for or related to, paxful.com at least three times between November 24, 2017 and November 27, 2017. This is further evidence of KVASHUK researching matters relevant to the fraud at the approximate time that the fraud scheme ramped up dramatically.

65. As part of my investigation, I analyzed the value of bitcoin (in United States dollars) deposited into KVASHUK's Coinbase account and compared it to the purchases and redemptions of CSV.[13] I was able to determine that, while significantly lower, the value of the bitcoin deposits to KVASHUK's Coinbase account generally correlated with the value of the purchased and redeemed CSV. The reasons for the lower value could include KVASHUK selling the CSV at a discount, bitcoin's general decline in value during early 2018, or that not all of the proceeds from this scheme have been identified.

---

13 This analysis does not take into account the value of any CSV that was blacklisted by Microsoft.



66. KVASHUK has used his unexplained wealth to make significant purchases. In March of 2018, KVASHUK paid roughly $162,000 for a Tesla vehicle. A Tesla Model S with the vehicle identification number (VIN) 5YJSA1E40JF249750 (the "SUBJECT VEHICLE") was registered with the Washington Department of Licensing to KVASUK [sic] in April 2018.

67. According to title company records, in June of 2018, KV ASHUK bought a lakeside home in Renton (the SUBJECT LOCATION) for roughly $1.675 Million.

68. KVASHUK told Microsoft investigator Andrew Cookson, in an interview on May 16, 2018, that he had rented a new place since the last time they spoke. In truth, records obtained during that investigation show that he had accepted a purchase agreement for the SUBJECT LOCATION as of approximately April 1, 2018, and a rental agreement to occupy the property prior to closing dated April 19, 2018. Email messages from Amazon.com to KVASHUK show pur-

chases of items to be delivered to him at the SUBJECT LOCATION as early as April 24, 2018.

69. Surveillance conducted on the SUBJECT LOCATION has repeatedly identified a Honda Insight parked in front of the house, including as recently as June 28, 2019. According to Washington Department of Licensing records, KVASHUK is listed as a registered owner for the vehicle.

False Tax Returns

70. On or about February 24, 2018, KVASHUK electronically filed a 2017 Form 1040, *US. Individual Income Tax Return,* with the IRS. The tax return appears to have been self-prepared by KVASHUK using the website 1040.com. The tax return reported income of $109,440 from wages, and net gains of $4,663 from the sale of various cryptocurrencies, including bitcoin, for total reported income of $114,103. Deposits into KVASHUK's Wells Fargo bank account *5789 in 2017 totaled $139,680.76.

71. On or about February 21, 2019, a 2018 Form 1040, *U.S. Individual Income Tax Return,* was filed electronically for KVASHUK by Tax Rite, Inc. The tax return was prepared by a paid return preparer. The tax return reported income of $76,927 from wages, $9,968 from dividends, and a loss of $71,745 (limited to a deductible loss of $3,000) from the sale of investments and cryptocurrency, including bitcoin, for total reported income of $83,895. Deposits into KVASHUK's Wells Fargo bank account *5789 in 2018 totaled $2,925, 374.48.

72. As shown above, KVASHUK, through his scheme to defraud Microsoft, acquired CSV totaling

approximately $971,161.26 in 2017 and $7,385,730.04 in 2018 at no cost to himself These amounts are includable in his gross income, and are taxable in the year they are received.

73. KVASHUK did report the income from the sales of bitcoin to Coinbase discussed above. However, in 2017 he only reported a taxable gain (sales price less basis) of approximately $1,547 in 2017 and a loss of approximately $69,418 in 2018. The limited gain and the loss reported on the tax returns appear to be the result of KVASHUK using the value of the bitcoin at the time he deposited them into his Coinbase account as his basis. In truth, because the bitcoin were obtained as proceeds of his scheme to defraud, and since KVASHUK did not report the income from his scheme to defraud, his basis in the bitcoin should have been $0. If this were the case, he would have had income from the sale of bitcoin obtained through the scheme of $47,715 in 2017 and $2,846,041 in 2018, based on the sales proceeds reported on his respective tax returns.

74. On December 19, 2017, KVASHUK emailed J.P. from taxhotline.net. Based on the context of the email, it appears to be a follow-up discussion to a prior phone call. In the message, KVASHUK indicated he was receiving gifts from his father in the form of bitcoin and questioned how to show on a tax return that the funds were a gift so he wouldn't "have any troubles in the future." He specifically noted that his father purchased the bitcoin with cash, and therefore had no records of the purchase.

75. On February 5, 2019, KVASHUK emailed D.L., his tax return preparer, regarding the preparation of KVASHUK's 2018 tax return. In the email, he told D.L. that his father sent him bitcoin, which he sold to

Coinbase for cash, and references a computer file that appears to be a report from Coinbase regarding transactions conducted in his Coinbase account. Based on my review of the tax return, the proceeds from bitcoin sales reported on the tax return reconcile to the U.S. currency withdrawn from Coinbase, and the cost basis claimed materially reconciles to the U.S. dollar value recorded by Coinbase at the time the bitcoin was deposited to KVASHUK's account.

76. As discussed above, while conducting blockchain analysis on the bitcoin deposited into KVASHUK's Coinbase account, I was able to determine that the majority of the bitcoin appeared to trace back to Paxful.com and Chipmixer.com.

77. Additionally, an email between KVASHUK and his father on May 18, 2018 includes copies of a 2018 non-immigrant visa application for KVASHUK's father which stated his father was a university lecturer with a monthly income of 30,000 in. Ukranian currency. Based on the exchange rate on that day, this would be approximately $1,156 per month.

PROBABLE CAUSE REGARDING THE PLACES TO BE SEARCHED

79. As set forth above, there is probable cause to believe that evidence of the offenses of mail fraud, wire fraud, money laundering, and tax fraud may be found in the locations to be searched.

80. Based on my training and experience, people often keep personal, financial, and tax records in their home. KVASHUK listed the SUBJECT LOCATION as his residence on his 2018 tax return.

81. According to records received from Comcast, KVASHUK received internet service at the SUBJECT LOCATION. Their records show this internet service was assigned the IP address 73.109.141.71 from at least November 22, 2018 through January 23, 2019. According to these records, this IP address was scheduled to remain assigned to this service through May 17, 2019 (after which Comcast may have either re-assigned that IP address, or assigned a new one, as Comcast typically assigns IP addresses for a sixth month period). Records obtained through the course of the investigation have identified this IP address being used to access KVASHUK's Coinbase account, KVASHUK's Gmail email account, KVASHUK's PayPal account, KVASHUK's Poloniex cryptocurrency account, KVASHUK's Blockchain.info cryptocurrency account, and KVASHUK's Microsoft store account (associated with his email address kvashuk.volodymyr@gmail.com). These account accesses occur beginning April 28, 2018 and continuing through April 29, 2019. The use of this IP address to access online accounts is indicative of digital devices being at the SUBJECT LOCATION.

82. According to Washington Department of Licensing records reviewed on June 13, 2019, the SUBJECT VEHICLE is registered to the SUBJECT LOCATION. In the past week agents have seen KVASHUK driving the SUBJECT VEHICLE at the SUBJECT LOCATION.

83. Based on my training and experience, I know that many people generally keep their cell phones and other digital devices on their person, in their home, in their vehicle, or in other places under their dominion and control. KVASHUK appears to regularly park his car in his garage; a relatively secure location that

makes it more likely that he would at least briefly store digital devices in the vehicle. The crimes in this case were committed almost entirely via digital devices, and thus there is probable cause to believe that evidence will be found on digital devices which may be stored in the vehicle.

84. According to records provided by Google, KVASHUK has a Samsung phone that has been active and associated with his Gmail account from August 2017 through at least May 1, 2019. Location records received from Google often place this phone at the SUBJECT LOCATION, including during evening hours when people are usually at home, from at least April 23, 2018 through April 28, 2019[14].

85. A bitcoin "Private Key" is essentially a password allowing the holder to spend bitcoin held at a bitcoin address with an associated "Public Key." Since anyone that has access to a Private Key can control the bitcoin located in the associated address, the security of a Private Key is very important. Based on my training and experience, I know that Private Keys, or the means to calculate a Private Key, may be stored either in a digital format or written down. I also know that people often keep Private Key information on their phones, computers, or in their homes.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

86. As described above and in Attachment B, this application seeks permission to search for evidence,

---

[14] The search warrant to Google for location data was obtained April 29, 2019. April 28, 2019 was the most recent date for which location data was provided.

fruits and instrumentalities that might be found at the SUBJECT LOCATION, in whatever form they are found. One form in which the evidence, fruits, and/or instrumentalities might be found is data stored on digital devices[15] such as computer hard drives or other electronic storage media.[16] Thus, the warrant applied for would authorize the seizure of digital devices or other electronic storage media or, potentially, the copying of electronically stored information from digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

87. Probable cause. Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and computer forensics examiners, and my training and experience, I submit that if a digital device or other electronic storage media is found at the SUBJECT LOCATION, in the SUBJECT VEHICLE, or on KVASHUK's person, there is probable cause to believe that

---

[15] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related. communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

[16] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

evidence, fruits, and/or instrumentalities of the crimes of wire fraud, mail fraud, money laundering, and filing false tax returns will be stored on those digital devices or other electronic storage media. As described above, information developed through the course of this investigation has shown that digital devices or other electronic storage media were used to access the Microsoft's online store, set up and access email accounts, conduct online research in furtherance of the scheme, purchase and redeem CSV, communicate with one or more tax preparers, and conduct bitcoin transactions. There is, therefore, probable cause to believe that evidence, fruits and/or instrumentalities of the · crimes of wire fraud, mail fraud, money laundering, and filing false tax returns exists and will be found on digital devices or other electronic storage media at the SUBJECT LOCATION, SUBJECT VEHICLE, and on KVASHUK's person, 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 preserved (and consequently also then recovered) for months or even years after they have been downloaded onto a storage medium, deleted, or accessed or viewed via the Internet. Electronic files downloaded to a digital device or other electronic 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 digital device or other electronic storage media, 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 digital device or other electronic 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."

88. Based on actual inspection of email messages, cryptocurrency transactions, and tax returns, I am aware that digital devices and other electronic storage

media were used to generate, store, and transmit documents and other information used in the wire fraud, tax evasion, and money laundering schemes. There is reason to believe that there is a computer system currently located at the SUBJECT LOCATION.

89. 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 digital devices or other electronic storage media 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 digital devices or other electronic storage media located at the SUBJECT LOCATION, in the SUBJECT VEHICLE, or on KVASHUK's person because:

a. Stored data can provide evidence of a file that was once on the digital device or other electronic storage media 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 digital device or other electronic storage media that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the history of connections to other. computers, the attachment of peripherals, the attachment

of USB flash storage devices or other external storage media, and the times the digital device or other electronic storage media was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

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 inculpating or exculpating the computer owner and/or others with direct physical access to the computer. 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.[17] 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

---

[17] For example, if the examination of a computer shows that: a) at 11:00am, someone using the computer used an internet browser to log into a bank account in the name of John Doe; b) at 11:02am the internet browser was used to download child pornography; and c) at 11:05 am the internet browser was used to log into a social media account in the name of John Doe, an investigator may reasonably draw an inference that John Doe downloaded child pornography.

timeline information described herein may either inculpate 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 digital device or other electronic storage media works can, after examining this forensic evidence in its proper context, draw conclusions about how the digital device or other electronic storage media 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 digital device or other electronic storage media 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, digital 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 digital device or other electronic storage media 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. 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.

90. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress KVASHUK's thumb and/or fingers on the device(s) that agents have probable cause to believe eithers belongs to him, or that he has access to, and (2) hold the device(s) that agents have probable cause to believe belong to him in front of his face, with each of his eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

DIGITAL DEVICES AS INSTRUMENTALITIES OF THE CRIMES

91. Digital devices were used as instrumentalities throughout several parts of the scheme. Specifically, digital devices were used (among other things) to create the pikimajado@tinoza.org and xidijenizo@axsup.net email addresses, create and access Microsoft online store accounts, "purchase" CSV through Microsoft

store test accounts, redeem CSV through the Microsoft store, order video cards through the Microsoft store, and conduct bitcoin transactions with the proceeds from the scheme.

PAST EFFORTS TO OBTAIN THIS EVIDENCE

92. Search warrants were obtained for information associated with various email accounts used in this scheme on April 29, 2019. Information obtained from these search warrants included content of stored email messages, web search history, cell phone location history, subscriber details, and related information.

93. The evidence sought through this search warrant has not been previously available to me or other agents, apart from the information described above.

RISK OF DESTRUCTION OF EVIDENCE

94. I know based on my training and experience that digital information can be very fragile and easily destroyed. Digital information can also be easily encrypted or obfuscated such that review of the evidence would be extremely difficult, and in some cases impossible. In the instant case, I know based on KVASHUK's internet search history that he may use encryption on the computer systems he utilizes to engage in his crimes. For example, on multiple dates in November and December 2017, KVASHUK searched for information on sending encrypted messages. On December 14, 2019, KVASHUK searched for information on encrypting flash drives. If an encrypted computer is either powered off or if the user has not entered the encryption password and logged onto the computer, it is likely that any information contained

on the computer will be impossible to decipher. If the computer is powered on, however, and the user is already logged onto the computer, there is a much greater chance that the digital information can be extracted from the computer. This is because when the computer is on and in use, the password has already been entered and the data on the computer is accessible. However, giving the owner of the computer time to activate a digital security measure, pull the power cord from the computer, or even log off of the computer could result in a loss of digital information that could otherwise have been extracted from the computer.

REQUEST FOR AUTHORITY TO CONDUCT OFF-SITE SEARCH OF TARGET COMPUTERS

95. Necessity of seizing or copying entire computers or storage media. In most cases, a thorough search of premises for information that might be stored on digital devices or other electronic storage media often requires the seizure of the physical items and later off-site review consistent with the warrant. In lieu of removing all of these items from the premises, it is sometimes possible to make an image copy of the data on the digital devices or other electronic storage media, onsite. Generally speaking, imaging is the taking of a complete electronic picture of the device'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 item, 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 on premises 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 the respective digital device and/or electronic storage media to obtain evidence. Computer hard drives, digital devices and electronic 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. Digital devices or other electronic storage media 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 on the premises. However, taking the items off-site and reviewing them in a controlled environment will allow 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 electronic storage media formats and on a variety of digital devices that may require off-site reviewing with specialized forensic tools.

SEARCH TECHNIQUES

96. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging, or otherwise copying digital devices or other electronic storage media that reasonably appear capable of containing some or all of the data or items that fall within the scope of Attachment B to this Affidavit, and will specifically authorize a later review of the media or information consistent with the warrant.

97. Because other people are believed to share the SUBJECT LOCATION as a residence, it is possible that the SUBJECT LOCATION will contain digital devices or other electronic storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found on those computers, this application seeks permission to search and if necessary to seize those computers as well. It may be impossible to determine, on scene, which computers contain the things described in this warrant. In the event that it can be determined that a digital device is used solely by individuals not associated with the scheme, a new search warrant will be obtained prior to seizing and searching the device.

98. Consistent with the above, I hereby request the Court's permission to seize and/or obtain a forensic image of digital devices or other electronic storage media that reasonably appear capable of containing data or items that fall within the scope of Attachment B to this Affidavit, and to conduct off-site searches of the digital devices or other electronic storage media and/or forensic images, using the following procedures:

Processing the Search Sites and Securing the Data.

a. Upon securing the physical search site, the search team will conduct an initial review of any digital devices or other electronic storage media located at the locations described in Attachments A-1, A-2, and A-3 that are capable of containing data or items that fall within the scope of Attachment B to this Affidavit, to determine if it is possible to secure the data contained on these devices onsite in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

b. In order to examine the electronically stored information ("ESI") in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of any digital device or other electronic storage media that is capable of

containing data or items that fall within the scope of Attachment B to this Affidavit.[18]

c. A forensic image may be created of either a physical drive or a logical drive. A physical drive is the actual physical hard drive that may be found in a typical computer. When law enforcement creates a forensic image of a physical drive, the image will contain every bit and byte on the physical drive. A logical drive, also known as a partition, is a dedicated area on a physical drive that may have a drive letter assigned (for example the c: and d: drives on a computer that actually contains only one physical hard drive). Therefore, creating an image of a logical drive does not include every bit and byte on the physical drive. Law enforcement will only create an image of physical or logical drives physically present on or within the subject device. Creating an image of the devices located at the search locations described in Attachments

---

[18] The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

A-1, A-2, and A-3 will not result in access to any data physically located elsewhere. However, digital devices or other electronic storage media at the search locations described in Attachments A-1, A-2, and A-3 that have previously connected to devices at other locations may contain data from those other locations.

d. If based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site image within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices or other electronic storage media will be seized and transported to an appropriate law enforcement laboratory to be forensically imaged and reviewed.

Searching the Forensic Images.

a. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope

of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit. Those techniques, however, may necessarily expose many or all parts of a hard drive to human inspection in order to determine whether it contains evidence described by the warrant.

b. Agents may utilize hash values to exclude certain known files, such as the operating system and other routine software, from the search results. However, because the evidence I am seeking does not have particular known hash values, agents will not be able to use any type of hash value library to locate the items identified in Attachment B.

REQUEST FOR SEALING

99. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. This is an ongoing investigation, and the target does not know the details of what investigators have learned and what evidence has been gathered. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness by resulting in the flight of the target, the destruction of evidence, transfer or concealment

of proceeds, or the intimidation or influencing of witnesses.

CONCLUSION

100. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of the crimes of mail fraud, wire fraud, money laundering, and filing of false tax returns are located at the SUBJECT LOCATION, in the SUBJECT VEHICLE, and on KVASHUK's person, as more fully described in Attachments A-1, A-2, and A-3 to this Affidavit, as well as on and in any digital devices or other electronic storage media found therein. I therefore request that the Court issue a warrant authorizing a search of the SUBJECT LOCATION, SUBJECT VEHICLE, and KVASHUK's person, as well as any digital devices and electronic storage media located therein, for the items more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such items found therein.

/s/ Eric Hergert
Special Agent,
Internal Revenue Service

SUBSCRIBED and SWORN to before me this 11th day of July, 2019.

/s/ Michelle L. Peterson
United States Magistrate Judge

ATTACHMENT A-1
LOCATION TO BE SEARCHED

The SUBJECT LOCATION is the residence and surrounding property located at 6409 Ripley Lane SE, Renton, WA 98056. The residence is a multi-story, single family residence located at the north end of Ripley Lane SE. The building has reddish wood grain and blue siding, a green metal roof, and the numbers 6409 on the south facing, southeast corner.

ATTACHMENT A-2
VEHICLE TO BE SEARCHED

The SUBJECT VEHICLE is a Tesla with the VIN 5YJSA1E40JF249750. According to Washington Department of Licensing records, the vehicle is registered to VOLODYMYR KVASHUK at 6409 Ripley Lane Southeast, Renton, Washington, 98056. Department of Licensing records identify the vehicle as a Tesla 2018 Model S sedan with the Washington license plate number BJW9291.

ATTACHMENT A-3
PERSON TO BE SEARCHED

The person of VOLODYMYR KVASHUK. VOLODYMYR KVASHUK is a twenty-five year old male, born on November 24, 1993 in the Ukraine. According to his Washington State Driver's License, he is six feet, one inch tall, weighs 175 pounds, and has brown eyes.

The search of VOLODYMYR KVASHUK shall include any and all clothing and personal belongings, including any digital devices, backpacks, wallets, briefcases, and bags that are in his physical possession, or within his immediate vicinity and control at the location where the search warrant is executed.

ATTACHMENT B
ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute evidence, instrumentalities, or fruits of violations of Mail Fraud, in violation of Title 18, United States Code, Section 1341, Wire Fraud, in violation of Title 18, United States Code, Section 1343, Money Laundering, in violation of Title 18, United States Code, Sections 1956(a)(1) and 1957, and Filing a False Tax Return, in violation of Title 26, United States Code, Section 7206:

1. All records relating to violations of the above statutes and involving VOLODYMYR KVASHUK, including:

a. Indicia of residence, ownership, control, or use of the SUBJECT LOCATION, the SUBJECT VEHICLE, cryptocurrency wallets and addresses, Microsoft CSV or gift card information, email accounts, bank and other financial accounts, and digital devices;

b. Evidence of use of the Microsoft online store, including usernames, passwords, or other login information, associated email addresses,

dates and times of access, items purchased, and device ID information;

c. Material related to Microsoft's testing program for its online store;

d. Evidence of research or communications, including online research, in furtherance of the crimes;

e. Stored records, communication, and related information regarding the source, acquisition, use, transfer, or disposition of CSV, gift cards, cryptocurrency, or potential proceeds of the fraud, in any form;

f. Evidence of use of virtual private networks, virtual machines, encryption, temporary email accounts, or bitcoin mixers;

g. Evidence of communication, access of websites, transactions conducted, and related information with 3rd party resellers or peer-to-peer transfers of CSV or gift cards;

h. Tax returns, workpapers, supporting documents, communication regarding the preparation of tax returns or tax regulations, procedures, or laws, and information regarding research or knowledge of tax regulations, procedures, or laws;

i. All bank records, checks, credit card bills, account information, tax returns, and other financial records, including records showing the source, deposit, withdrawal, transfer, or disposition of scheme proceeds;

j. All cryptocurrency wallets, to include current balance and transaction history, or information that could be used to reconstruct cryptocurrency transaction history, whether included in a cryptocurrency wallet file or separate, in either digital or paper form;

k. Evidence of use of other names, including but not limited to "Grigor Shikor" and "Vladamir," along with alternate spellings of these names;

l. GeForce GTX 1070 computer video cards; and

m. Evidence related to the finances of members of KVASHUK's s family who are a possible source of funds or income.

2. Digital devices[1] or other electronic storage media[2] and/or their components, which include:

---

[1] Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/ digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

[2] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks. RAM. floppy disks. flash memory. CD-ROMs. and other magnetic or optical media.

a. Any digital device or other electronic storage media capable of being used to commit, further, or store evidence of the offenses listed above;

b. Any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

3. Any digital devices or other electronic storage media that were or may have been used as a means to commit the offenses described on the warrant, including devices used to:

a. obtain, redeem, or transfer Microsoft CSV, gift cards, or similar information;

b. access the Microsoft online store, Private Internet Access, or other virtual private networks;

c. communicate with, or access 3rd party CSV or gift card reseller websites;

d. access email accounts associated with the scheme, or created and accessed temporary email accounts;

e. conduct cryptocurrency transactions, including creating accounts, transferring cryptocurrency, and selling cryptocurrency;

f. conduct financial transactions or store financial information, prepare tax returns or supporting information, or communicate with tax return preparers.

4. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant, and in addition to the items set forth in 1(a)-1(m), above:

a. evidence of who used, owned, or controlled the digital device or other electronic storage media 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 digital device or other electronic storage media, 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 of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

f. evidence of the times the digital device or other electronic storage media was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

h. documentation and manuals that may be necessary to access the digital device or

other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

i. contextual information necessary to understand the evidence described in this attachment.

5. Records and things evidencing Internet Protocol addresses used to access the internet, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. records of Internet Protocol addresses used;

c. records of 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;

d. records of Virtual Private Network (VPN) software or use; or use of a proxy service; and

e. records related to Device Identification Numbers.

6. During the execution of this search warrant, law enforcement is permitted to: (1) depress KVASHUK's thumb and/or fingers on the device(s) that agents have probable cause to believe belong to him; and (2) hold the device(s) that agents have probable cause to believe belong him in front of his face, with each of his eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device

in front of a person's face, law enforcement may not use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.