FOR PUBLICATION

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 OPINION

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

Argued and Submitted October 7, 2021
Seattle, Washington

Filed March 28, 2022

Before: Richard A. Paez, Milan D. Smith, Jr., and Jacqueline H. Nguyen, Circuit Judges.

Opinion by Judge Nguyen

SUMMARY*

Criminal Law

The panel affirmed Volodymyr Kvashuk's conviction on 18 fraud-related counts in a case in which Kvashuk stole $10 million in digital gift cards from his employer, Microsoft, using login credentials he filched from his coworkers.

Kvashuk challenged the denial of his motion to suppress evidence seized from his house on the ground that the search warrant lacked probable cause, arguing that the warrant affidavit failed to establish a nexus between the unlawful activities and the places to be searched. Considering the totality of the circumstances, the panel concluded that the search warrant affidavit showed a fair probability that evidence of Kvashuk's crimes would be found on a computer at his residence, and that there was therefore an adequate nexus between the unlawful activities and the place to be searched. The panel rejected Kvashuk's argument that the evidence supporting the application was stale. Rejecting Kvashuk's challenge to the district court's denial of his request for a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978), the panel wrote that Kvashuk identified no false or misleading statement in the affidavit, let alone one that the affiant made intentionally or recklessly.

Kvashuk contended that his two convictions for aggravated identity theft, which stem from his use of coworkers' accounts intended for testing the Microsoft Universal Store, are infirm because the test accounts do not

* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

constitute a "means of identification" under 18 U.S.C. § 1028A(a)(1), in that the accounts do not "identify a specific individual." Rejecting this contention, the panel wrote that the test accounts' purpose, prerequisites, and functionality do not bear on whether they "identify a specific individual"; that the test accounts here could be and did identify specific employees; and that the Universal Store team's limited sharing of test accounts and passwords was insufficient to differentiate the test accounts from any other business email account associated with a specific person.

Kvashuk contended that the district court violated his due process rights by preventing him from presenting a complete defense—in particular, by excluding evidence of his status in the United States as an asylum applicant from Ukraine. He argued that his sole defense to the prosecution's theory that he used crypto currency to conceal the money trail from his crime was that he did not intend to defraud Microsoft but used Bitcoin as an asylum seeker to avoid detection by the Ukrainian government. The panel wrote that while testifying about his asylum status might have strengthened his defense that he did not defraud Microsoft, Kvashuk was able to raise the defense without it. The panel held that the district court did not abuse its discretion in concluding 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 he could suffer immigration consequences if convicted on the charges.

Kvashuk contended that the district court should have dismissed a juror because the juror had experience with the Universal Store team. The panel wrote that merely working for the same large organization as the defendant is an insufficient basis for implied bias, and concluded that

because the juror's personal experience on the Universal Store team was not similar or identical to the fact pattern at issue in the trial, the district court properly denied the motion to remove him.

COUNSEL

Joshua Sabert Lowther (argued), Lowther Walker LLC, Atlanta, Georgia, for Defendant-Appellant.

Michael Dion (argued), Assistant United States Attorney; Tessa M. Gorman, Acting United States Attorney; United States Attorney's Office, Seattle, Washington; for Plaintiff-Appellee.

OPINION

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 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

[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.

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.

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.

[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.

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.

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]

[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.

[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.

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 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

---

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.

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 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.

[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.

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 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

[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).

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

[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

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 activities 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

a clear pattern of deposits into Kvashuk's Coinbase account that followed redemption of the stolen CSV.

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) 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

[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.

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 misleading 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 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 . . . .

[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).

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.