

NOT TO BE PUBLISHED IN THE OFFICIAL REPORTS

California Rules of Court, rule 8.1115(a), prohibits courts and parties from citing or relying on opinions not certified for publication or ordered published, except as specified by rule 8.1115(b). This opinion has not been certified for publication or ordered published for purposes of rule 8.1115.

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SECOND APPELLATE DISTRICT

DIVISION EIGHT

THE PEOPLE,

Plaintiff and Respondent,

v.

KAVEH KHALEGHI,

Defendant and Appellant.

B254145

(Los Angeles County
Super. Ct. No. BA390776)

APPEAL from a judgment of the Superior Court of Los Angeles County,
Michael Garcia, Judge. Affirmed.

Doreen B. Boxer, under appointment by the Court of Appeal, for Defendant and
Appellant.

No appearance for Plaintiff and Respondent.

Kaveh Khaleghi pled no contest to one count of grand theft pursuant to Penal Code¹ section 487, subdivision (a) after his motion to suppress was denied. Khaleghi's appointed counsel filed an opening brief raising no issues pursuant to *People v. Wende* (1979) 25 Cal.3d 436 (*Wende*). After being notified of his right to file a supplemental brief, Khaleghi submitted a 45-page document, in which he contends the denial of his suppression motion was reversible error because the three search warrants leading to the seizure of the evidence incriminating him were impermissibly overbroad. Having found no arguable issues exist and finding no merit to Khaleghi's contentions, we affirm the judgment.

FACTS

In 2011, the Los Angeles District Attorney's Office began an investigation which ultimately led to multiple counts of theft, embezzlement, and money laundering against Khaleghi for perpetrating a fraudulent scheme against foreign companies through his business, ComputerWide. One of Khaleghi's victims was Georgia Solomou, who owned MedIT, a company operating in the country of Cyprus. In an interview with investigator Michael Deck on February 18, 2011, Solomou reported she wired over \$85,000 to ComputerWide for the purchase of computer equipment in 2010, which she never received. In a similar transaction, a German company, Timlic, wired over \$200,000 to ComputerWide in approximately April 2010 for the purchase of networking equipment, which it never received.

On March 9, 2011, Deck submitted an affidavit for a search warrant of certain IP addresses he believed would uncover the individuals controlling ComputerWide and their physical address. Deck explained that "[a]n IP address is a unique identifier much like a residential address for mail." One particular IP address 68.183.173.229 was maintained by an internet service provider known as DSL Extreme, which Deck believed kept records of subscriber information for that IP address. IP address 68.183.173.229 appeared on the email communications ComputerWide exchanged with Solomou. Two

¹ All further section references are to the Penal Code unless otherwise specified.

other IP addresses 67.18.44.20 and 74.52.124.98 were also gleaned from the email communications between ComputerWide and Solomou. Deck tracked the IP addresses to computer servers maintained by Websitewelcome.com, which stored all of ComputerWide's emails. According to Deck, "[t]he emails and other requisite information are necessary evidence to corroborate information and identify suspects and additional victims." Additionally, Deck sought a warrant for the search of bank records related to the bank account into which Solomou wired her payment as well as the records of the phone numbers given to Solomou by ComputerWide.

Search warrant number 6174 was issued on March 9, 2011, to DSL Extreme, websitewelcome.com, The Planet.com Internet Services, Inc., JP Morgan Chase Bank, N.A., Verizon Wireless and Paetec Communications, Incorporated for information from "January 1, 2010 to present" related to the bank accounts, cell phone numbers, and IP addresses collected from Deck's investigation.

After further investigation, Deck was able to obtain Khaleghi's identity and physical address. A second warrant number 61810 was issued on March 23, 2011, to search Khaleghi's person, residence, and car for "[a]ll documentation in connection with ComputerWide, MedIT, Timlic, Cotewa, Georgia Solomou, Harald Suender, and Manuel Wannemacher; corporation records, fictitious business records, and business licenses for ComputerWide; documentation identifying suppliers of computers, computer parts, and networking equipment; invoices, purchase agreements, and receipts between ComputerWide, customers, and suppliers of computers and computer related equipment; documentation identifying customers of Computer Wide; address books and contact lists, any item tending to establish domain or control of ComputerWide. [¶] Employee records for "Will" or William Ravi. [¶] Telephone records for [three phone numbers]. [¶] All bank and other financial documents, including tax records for ComputerWide, Kaveh Khaleghi, and Hesmat Ravaei. [¶] U.S. or foreign currency. [¶] Any item

tending to show domain or control of the premises, such as utility bills and mail. [¶] All passports.”²

In the accompanying affidavit, Deck stated, “I know from my training and experience in investigating fraud related crimes, it is common for suspects to hide their assets. Often they will open bank accounts in their family member names and other business names. Banking records for ComputerWide, Khaleghi, and Ravaei are necessary to track the flow of money, identify additional victims, aid in restitution, and determine the loss suffered by the victims. [¶] . . . [¶] Furthermore, I am requesting tax records for ComputerWide, Khaleghi, and Ravaei be seized at the location. These records are necessary to show a basis of income possibly not reported to the IRS and other crimes. The records will possibly show other assets not known to help aid in restitution.” Deck further stated that one of the victims “has since learned from others in the business that ComputerWide is notorious for sending emails about computer equipment they have in stock and when someone agrees to a purchase, nothing good happens as a result.” Deck revealed that Khaleghi was being deported and believed that led him to defraud the victims, knowing he would not be in the country to be prosecuted. As a result, he requested seizure of his and his mother’s passports to prevent flight.

Deck also tracked the misappropriated funds to Las Vegas Casinos. “A review of the JP Morgan Chase Bank records for ComputerWide revealed a pattern between the aforementioned victims and their wire transfers to ComputerWide and ComputerWide’s subsequent transfer of funds to Las Vegas casinos, payments of other debts, and cash withdrawals.” As a result, Deck submitted an application and affidavit for a search warrant through the Las Vegas Metropolitan Police Department for a search of Khaleghi’s records in various casinos in Las Vegas, Nevada, including the Wynn, the Cosmopolitan, and the Aria. Deck believed the casino records would show a pattern of

² MedIT, Timlic, Cotewa, Georgia Solomou, Harald Suender, and Manuel Wannemacher are the individuals and companies who fell victim to ComputerWide’s fraud. Heshmat Ravaei is Khaleghi’s mother; she was listed as ComputerWide’s president and as the subscriber for the IP address found on ComputerWide’s emails. Solomou spoke with a ComputerWide salesman named Will Ravi.

gambling and “possible tax violations” and would assist in tracking and recovering the victims’ money. The application for search warrant submitted through the Las Vegas Metropolitan Police Department was approved on September 22, 2011, by Judge Brian Rutledge authorizing a search for the casinos’ records of Khaleghi from January 1, 2007 to the “present.”³

Khaleghi was arrested on January 12, 2012. He was charged with seven counts of grand theft (§ 487, subd. (a)), two counts of embezzlement (§ 506), seven counts of money laundering (§ 186.10, subd. (a)(2)), and one count of tax evasion (Revenue & Taxation Code, § 19706) with sentencing enhancement allegations relating to the amount of money involved.

Khaleghi moved to suppress the evidence seized on the grounds probable cause did not exist to support issuance of the warrants, the warrants were insufficient and overbroad, and the property or evidence obtained was not described in the warrants. The prosecutor declined to file a written opposition, but argued at the hearing that the warrants were supported by probable cause and were sufficiently particular in who and what was to be searched. The prosecutor described the warrants and the affidavit as “fairly standard.” The trial court agreed and denied the motion to suppress on December 2, 2013.

Khaleghi thereafter entered a no contest plea to one count of grand theft of personal property in violation of section 487, subdivision (a). After a waiver under *People v. Harvey* (1979) 25 Cal.3d 754, 758, the remaining counts were dismissed. Khaleghi was sentenced to three years in county jail pursuant to section 1170, subdivision (h)(1) and (h)(2). He was also ordered to pay a total of \$831,000 to his various victims pursuant to the plea agreement. He timely appealed.

³ A separate warrant number 63062 authorizing a search of the casinos for Khaleghi’s records was issued by California Superior Court Judge Shelly Torrealba on September 22, 2011. Khaleghi asserts a California court has no authority to issue a search warrant to entities based in Nevada. We need not reach this issue as the record contains a copy of the warrant application submitted by the Las Vegas Metropolitan Police Department which was approved by a Nevada judge.

DISCUSSION

Khaleghi's appointed counsel filed an opening brief raising no issues pursuant to *Wende, supra*, 25 Cal.3d 436. Our independent review has revealed no arguable issues. Nonetheless, we address the issues raised in Khaleghi's 45-page supplemental brief. As far as we can decipher, Khaleghi's somewhat rambling brief argues the warrants were overbroad because Deck's affidavits only supported a search for evidence of the specific crimes and victims identified as well as the time periods during which these crimes occurred. We disagree.

Our Supreme Court has rejected the contention that there must be a precise correlation between the items in the warrant and the probable cause declarations in the affidavit. (*People v. Kraft* (2000) 23 Cal.4th 978, 1050.) The requirement of reasonable particularity "is a flexible concept, reflecting the degree of detail available from the facts known to the affiant and presented to the issuing magistrate." (*People v. Tockgo* (1983) 145 Cal.App.3d 635, 640; *Bryant, Smith and Wheeler* (2014) 60 Cal.4th 335, 370-371.) "[I]n a complex case resting upon the piecing together of 'many bits of evidence,' the warrant properly may be more generalized than would be the case in a more simplified case resting upon more direct evidence." (*People v. Bradford* (1997) 15 Cal.4th 1229, 1291, quoting *Andresen* (1976) 427 U.S. 463, 481, fn. 10.)

Given the purpose of the warrant, the nature of the items sought, and the total circumstances surrounding the case, we find the scope of the search was appropriate. We reject Khaleghi's position that searching officers must have probable cause to connect each item seized with a particular victim and a particular crime identified in the affidavit. There was probable cause to believe there were additional victims who may have been defrauded by ComputerWide over a longer period of time than that specified in Deck's affidavits. Deck stated in his affidavit that MedIT received email advertisements for several years from ComputerWide and that Solomou continued to receive email advertisements from ComputerWide up until March 2011. Moreover, the emails were widely disseminated. Deck was informed "that ComputerWide is notorious for sending

emails about computer equipment they have in stock and when someone agrees to a purchase, nothing good happens as a result.”

Deck’s affidavit demonstrated the reasonable likelihood that ComputerWide’s fraud extended beyond MedIT and Timlic. That possibility was borne out when additional victims were uncovered. This case is distinguishable from *Burrows v. Superior Court* (1974) 13 Cal.3d 238, 249-250 (*Burrows*), on which Khaleghi relies. In *Burrows*, there was no indication the lawyer misappropriated funds from anyone other than the one client and during any time other than his representation of the client. (*Ibid.*)

Even assuming the warrants were overbroad for lack of a clear time frame and nexus to the identified crimes and victims, the good faith exception created in *United States v. Leon* (1984) 468 U.S. 897 (*Leon*) applies to support denial of the suppression motion. The *Leon* good faith exception allows the introduction of evidence obtained under a defective warrant issued by a neutral and detached magistrate if the officers who executed the warrant acted in the reasonable good-faith belief that the warrant was valid. (*Id.* at p. 904.) Good faith is defined as an “objectively reasonable reliance.” (*Id.* at p. 920.) The affidavits supporting the warrants in this case document an extensive police investigation into ComputerWide’s transactions. The information discovered from each search provided probable cause for the subsequent search warrants. There is no evidence that the officers conducting the search did not believe the warrant was valid.

Khaleghi also challenges the admission of evidence found on his computer after he gave the police his password without a *Miranda*⁴ advisement. Likewise, he contends incriminating statements he made to the investigating officers should be quashed. There is no merit to these contentions. At the motion to suppress hearing, defense counsel conceded there was no evidence that Khaleghi’s statements were involuntary or that he was in custody at the time. She also agreed the matter was not before the court on the motion to suppress, but should be “the subject of a different motion.” That motion was never filed and the issue is forfeited.

⁴ *Miranda v. Arizona* (1966) 384 U.S. 436 (*Miranda*).

DISPOSITION

The judgment is affirmed.

BIGELOW, P.J.

We concur:

RUBIN, J.

GRIMES, J.