IN THE SUPREME COURT OF CALIFORNIA

THE PEOPLE,
Plaintiff and Respondent,
v.
SI H. LIU,
Defendant and Appellant.

S248130

Second Appellate District, Division Eight
B279393

Los Angeles County Superior Court
GA090351

November 21, 2019

Justice Cuéllar authored the opinion of the Court, in which Chief Justice Cantil-Sakauye and Justices Chin, Corrigan, Liu, Kruger, and Groban concurred.

PEOPLE v. LIU

S248130

Opinion of the Court by Cuéllar, J.

We retread in this case ground recently traveled in *People v. Romanowski* (2017) 2 Cal.5th 903 (*Romanowski*). At issue once more is how to assess the value of stolen access card information — a term encompassing information related to credit and debit cards, bank accounts, and similar financial devices. (See Pen. Code, § 484e, subd. (d) (section 484e(d)); *id.*, § 484d, subd. (2).)[1]

What we concluded in *Romanowski* is that courts conducting that analysis must do what they do in all theft cases: figure out "how much [the stolen property] would sell for." (*Romanowski*, *supra*, 2 Cal.5th at p. 915.) Discerning that amount is an endeavor that calls for some subtlety and may depend on more than one factor. Further complicating the inquiry in this context is the lack of a legal market for stolen access card information. But instead of engaging in that nuanced inquiry, the Court of Appeal here simply assumed that the value of what the defendant obtained using the stolen information sets a floor on the fair market value of the stolen access card information she unlawfully used. Because the Court of Appeal's reasoning falls short of what *Romanowski* requires, and because both parties agree that further factfinding is

---

[1] All statutory references are to the Penal Code unless otherwise noted.

necessary to resolve this case, we vacate the judgment and remand.

I.

Defendant Si H. Liu advertised loan services in local newspapers. Those offerings were a front for nefarious ends: Liu was running a fraudulent scheme targeting immigrants in the Los Angeles area. When unwitting readers sought help obtaining financing, Liu asked them for sensitive documents and information — such as driver's licenses and social security numbers — as well as credit and debit cards. She then went on personal spending sprees, sometimes by surreptitiously opening new lines of credit in her victims' names, but most often by simply charging purchases to their credit or debit card accounts. All told, Liu fraudulently charged thousands of dollars.

The law eventually caught up with Liu. The People charged her with nearly two dozen criminal counts related to her fraudulent activities. Those charges included burglary, unlawfully acquiring the personal identifying information of 10 or more people, and — most relevant here — theft of access card information under section 484e(d). At trial, a jury convicted Liu on all counts. The Court of Appeal reversed one of her convictions but affirmed the rest. Five of Liu's convictions for theft of access card information under section 484e(d) were among those upheld on appeal and they are at issue here.

In November 2014, while Liu's direct appeal was pending, California voters approved Proposition 47: The Safe Neighborhoods and Schools Act. To decrease the number of people in prison for nonviolent crimes, Proposition 47 reduced the punishment prescribed by law for a wide swath of crimes in California. Many offenses once punishable as felonies are now

treated as misdemeanors. Such crimes include, with a few exceptions not relevant here, "obtaining any property by theft where the value of the money, labor, real or personal property taken does not exceed nine hundred fifty dollars ($950)." (§ 490.2, subd. (a) (section 490.2(a)).) What's more, Proposition 47's changes apply not just to future offenders, but also to certain people currently serving prison sentences for past convictions. Someone who "would have been guilty of a misdemeanor" if Proposition 47 had "been in effect at the time of [his or her] offense" may seek relief. (§ 1170.18, subd. (a).) Specifically, a person in that position may "petition for a recall of sentence before the trial court that entered the judgment of conviction in his or her case" and "request resentencing in accordance with" Proposition 47's changes. (§ 1170.18, subd. (a); but see *People v. Lara* (2019) 6 Cal. 5th 1128, 1134 [those sentenced after Proposition 47 are entitled, under the provisions of that proposition, "to initial sentencing . . . and need not invoke the resentencing procedure"].)

After the Court of Appeal issued its decision in Liu's direct appeal, Liu petitioned the trial court for Proposition 47 relief. She sought resentencing on five of her convictions for theft of access card information. Her petition, which she filed pro se, argued that the value of the property she obtained was "not more than $950." After a brief hearing on Liu's petition for resentencing, the trial court denied the petition because Liu was "not eligible" for relief. The court did not elaborate.

Liu appealed the trial court's denial of her Proposition 47 petition. While that appeal was pending, we decided *Romanowski*. What we concluded is that theft of access card information under section 484e(d) qualifies as a "theft" offense under section 490.2(a) — and that Proposition 47 therefore

reduced such thefts to misdemeanors where " 'the value of the . . . property taken' " was less than $950. (*Romanowski*, *supra*, 2 Cal.5th at p. 917, quoting § 490.2(a).) The value of stolen access card information, we continued, means the same thing as it does for all theft offenses: " 'reasonable and fair market value.' " (*Romanowski*, at p. 914, quoting § 484, subd. (a) (section 484(a)).)

With the benefit of *Romanowski*, the Court of Appeal affirmed in part and reversed in part the trial court's pre-*Romanowski* denial of Liu's Proposition 47 petition. (*People v. Liu* (2018) 21 Cal.App.5th 143, 153 (*Liu*).) The Court of Appeal based its decision on the value of what Liu had obtained with her victims' access card information. (*Id.* at p. 149.) "Surely," the Court of Appeal explained, "stolen access card information would sell for *at least* the value of the property obtained by a defendant who used the information . . . ." (*Ibid.*, italics added.) Because the record established that Liu unlawfully obtained more than $950 using what she stole in relation to three of her convictions, the Court of Appeal affirmed the trial court's denial of Liu's petition on those counts. (*Ibid.*) But because the same could not be said for her other two convictions, the Court of Appeal reversed and remanded for further proceedings on those two counts. (*Ibid.*)

II.

We granted review to decide whether the Court of Appeal properly applied our decision in *Romanowski*. We conclude that it did not.

A.

Because theft of access card information in violation of section 484e(d) is a theft offense under section 490.2(a), we held

in *Romanowski* that courts must value stolen access card information just as they would any stolen property in a theft case. They must determine "a reasonable approximation of the stolen information's value, rather than the value of what (if anything) a defendant obtained using that information." (*Romanowski*, *supra*, 2 Cal.5th at p. 914.) That's because the value of property a defendant acquires using the illicitly obtained access card information "is punished as a separate crime" under section 484g. (*Ibid.*) Under that section, "the value of all money, goods, services, and other things of value obtained" by using stolen access card information determines the severity of the offense. (§ 484g.)[2]

Yet the same is not true for the offense at issue in this case: *theft* of access card information in violation of section 484e(d). For that offense, courts must calculate "how much stolen access card information would sell for" to determine whether it falls above or below the $950 threshold.[3] (*Romanowski*, *supra*, 2 Cal.5th at p. 915.) When performing this calculation, courts must determine the value of the information at the time of the "acqui[sition] or ret[ention]" of information on which criminal liability is based. (§ 484e(d).) Someone seeking relief under

---

[2] Besides being charged with the theft of access card information, Liu was charged with and convicted of three counts of grand theft by means of illegally obtained access card information in violation of section 484g. The Court of Appeal later reversed her conviction for one of those counts.

[3] Our decision about a forgery statute in *People v. Franco* (2018) 6 Cal.5th 433 does not affect our conclusion here. This case — like *Romanowski*, but unlike *Franco* — is "a theft case," not a forgery case. (*Franco*, at p. 438.) So it is *Romanowski*, not *Franco*, that governs.

Proposition 47, we concluded, bears the "ultimate burden" of showing she is eligible to receive it. (*Romanowski*, *supra*, 2 Cal.5th at p. 916.)

In *Romanowski* we acknowledged the "potential difficulty of putting a price on this property" (*id.* at p. 911) because the " 'fair market value' of stolen access card information," traded in illicit markets, "will not always be clear" (*id.* at p. 915). Unlike everyday retail products such as shoes or electronics, or data about human behavior harvested from the online activity of consenting users, unlawfully obtained access card information cannot be bought and sold legally. The utility of such information for obtaining merchandise or services, moreover, tends to be contingent rather than certain. As with the prize money one may glean from an earlier purchased lottery ticket, the ultimate worth of stolen access card information often depends on facts not known at the time of acquisition. Access card information can nonetheless be sold in illicit markets, and, with disturbing frequency, it is. That there exists no lawful market for this information, and often no clear sense of what it will purchase or for how long, may complicate the calculation of its fair market value. But as we held in *Romanowski*, any added complication "does not relieve courts of th[e] duty" to make that calculation. (*Ibid.*) To the contrary, "the possibility of illegal sales" of access card information is a key factor in the analysis — and one that warrants careful attention. (*Ibid.*)

The possibility of such sales — and ultimately, the value of the stolen access card data — tends to be driven by multiple factors. Consider the credit limit on a credit card or the account balance on a debit card. Assuming the unwitting fraud victim isn't continuing to pay down the credit card balance or replenishing the account balance, these values represent the

maximum amount someone possessing stolen access card information could charge to (or withdraw from) the victim's account. The higher the credit limit (or account balance), the more valuable the information — at least if the thief or potential purchaser of the data knows the limit (or balance) when she acquires the access card information. (See Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web* (Dec. 6, 2017) (Experian) <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> [as of November 19, 2019].)[4]

No matter how high the credit limit or account balance, would-be purchasers are unlikely to pay much for stolen account information unless they believe they can exploit it. So how readily, if at all, stolen access card information can be used matters. Someone will find it easier to make unauthorized charges if she has not just the card number and expiration date, but also the security code on the back (what's sometimes called a CVV2 code) and the card's billing ZIP code. One might thus place a premium on more detailed access card information, even if the relevant credit limit (or account balance) is lower. (Experian, *supra*; Franklin et al., An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants (2007) Online Credentials and Sensitive Data, p. 11 (Franklin) <http://www.icir.org/vern/papers/miscreant-wealth.ccs07.pdf> [as of November 19, 2019].)

But even such detailed information may not squelch fully the perils inherent in buying stolen access card information.

---

[4] All Internet citations in this opinion are archived by year, docket number, and case name at <http://www.courts.ca.gov/38324.htm>.

Such buyers bear the risk that their purchase will become — or already is — useless. Stolen credit and debit cards often get frozen or canceled, particularly when a cardholder or their financial institution catches a whiff of fraud. The value of stolen access card information may typically be discounted to account for these risks. And by that same principle, freshly stolen access card information may fetch a higher price than stale information because it is more likely to be active. (Franklin, *supra*, at p. 11; Ablon, et al. Markets for Cybercrime Tools and Stolen Data (2014) p. 11 (RAND) <https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf> [as of November 19, 2019].)

The dynamics of supply and demand matter for illegal markets, too, just as they do for legal ones. (Experian, *supra*; Franklin, *supra*, Inferring Global Statistics and Trends, at p. 12.) Suppose a hacker successfully attacks a major retailer and then puts information related to thousands of access cards up for sale online. The resulting supply glut may reduce (at least for a time) the illegal market price of comparable stolen access card information. (See RAND, *supra*, at p. 8.) In other words, the value of stolen access card information depends in no small part on how much comparable information is available on the illegal market — and how many people are looking to buy it. (See Black's Law Dict. (10th ed. 2014) p. 1785 [describing a "fair market value" as "the point at which supply and demand intersect"].)

These factors don't cover the waterfront of what a court may consider in determining whether a defendant's proposed valuation of stolen access card information is objectively reasonable. Nor do they encompass all of the methods useful in discerning the value of stolen access card information. But they

demonstrate that the inquiry *Romanowski* requires for determining the severity of a section 484e(d) offense — assessing how much the stolen access card information in question would sell for — is a nuanced endeavor.

The inquiry is nonetheless eminently feasible. Where the facts otherwise presented to the trial court don't already offer some bearing on this question, the best place to start may be consulting, perhaps with help from an expert witness, the current trends in illicit markets for stolen access card information and the prevailing price of illegally obtained comparable information. (See Peretti, *Data Breaches: What the Underground World of "Carding" Reveals* (2008) 25 Santa Clara Computer & High Tech. L.J. 375, 381–389, 412 [describing sophisticated online illegal market for stolen access card information]; Franklin, *supra*, at p. 1 [similar]; cf. *People v. Tijerina* (1969) 1 Cal.3d 41, 45 [noting "that the price charged by a retail store from which merchandise is stolen" is ordinarily "sufficient to establish the value of the merchandise" because it tends to "accurately reflect the value of the merchandise in the retail market"].) Such an expert might help identify what considerations are relevant to the fair market value analysis in any given case.

B.

The Court of Appeal sought to apply *Romanowski* on the thin record before it. But we conclude, as the parties agree, that this case should be remanded to the trial court for further factfinding in light of *Romanowski* and today's decision.

1.

What little evidence the record contains about the value of the access card information Liu stole consists of the amounts she

unlawfully charged to her victims' accounts. We agree such evidence may be considered — so long as it's done "with the goal of determining the [stolen access card information's] fair market value." (*Caretto v. Superior Court* (2018) 28 Cal.App.5th 909, 920.) Evidence of unauthorized charges may tend to show that someone could use the stolen information in question. And at least if the ability to make such charges was knowable when a defendant acquired the access card information, such charges may offer a clue as to how much value could be extracted from that information. Both facts could bear on the fair market value of stolen access card information.

But evidence of unauthorized charges — while conceivably relevant — does not, as the Court of Appeal assumed, set a floor on how much someone would be willing to pay for it. (See *Liu*, *supra*, 21 Cal.App.5th at p. 149.) That figure may be gleaned from using a range of methods and involves various factors, such as: (1) the access card's credit limit or the account balance, if knowable when the defendant engages in the acquisition or retention of information that serves as the basis for criminal liability under section 484e(d); (2) the amount of account information possessed by the defendant; (3) how much the value of the information has been diminished because of its sale in illicit markets; (4) how recently the information was stolen; and (5) the prevalence of comparable information on the illicit market. The extent to which these factors (and others) are relevant to calculating the fair market value of stolen access card information in any given case is a factual question.

The Court of Appeal assumed that unauthorized charges necessarily reflect the minimum fair market value of stolen access card information. That alluring assumption may simplify the inquiry. But it conflates the value of the access card

information itself with the value of the property obtained through use of the stolen access card information. Whereas the former is punished under section 484e(d), the latter, as we have noted, "is punished as a separate crime" under section 484g. (*Romanowski*, *supra*, 2 Cal.5th at p. 914.)

A hypothetical illustrates why the two values are not bound, or even especially likely, to be identical. Consider a defendant who maxes out a $10,000 credit limit using stolen access card data. Does "common sense" tell us that someone would have paid $10,000 for the stolen access card information he used? (*Liu*, *supra*, 21 Cal.App.5th at p. 149.) Would-be buyers in that situation might as well just hold on to their $10,000 in cash. Or they could go out and buy (legitimately) the $10,000 worth of goods they would have bought (fraudulently) using the stolen access card information. There would be little, if any, reason to go through the trouble of buying the stolen access card information.

Inherent in the codified concept of a "reasonable and fair market value" (§ 484(a)), moreover, is the notion that comparable property is of comparable worth. But the Court of Appeal's insistence that the fair market value of stolen access card information could be no lower than the value of the property obtained by a defendant using that information risks creating disparate valuations of similar stolen access card information. Consider two more hypothetical defendants. One is prudent and makes small purchases to avoid detection. The other is daring and makes big purchases to maximize her reward. Under the approach taken by the Court of Appeal, the latter defendant would face a drastically higher floor on the fair market value of the access card information she stole — even if she stole precisely the same information as her more prudent

counterpart. So such a doctrinal shortcut risks results that are irreconcilable with *Romanowski*.

2.

Having rejected the Court of Appeal's reasoning, we must now decide how to proceed with this case. On that question, the parties agree. They ask us to remand for further factfinding about the fair market value of the access card information Liu stole with respect to all of her section 484e(d) convictions. Indeed, the People concede it's "impossible to determine" whether the trial court concluded Liu was ineligible for relief because it: (1) thought that, contrary to our later decision in *Romanowski*, Proposition 47 didn't apply to violations of section 484e(d) at all; or (2) made a factual finding about the value of the stolen access card information at issue here. If anything, the People tell us, the record suggests the trial court did the former — and thus did *not* determine "the access cards' value, let alone [apply] the reasonable and fair market value test mandated" by *Romanowski*.

We share the People's impression about this record's inscrutability on the issue before us. The course suggested by the parties is therefore the right one. The trial court has yet to consider Liu's petition in light of *Romanowski*, and has not developed the record with an eye to making the factual findings *Romanowski* demands. The trial court should get that chance. We thus vacate the judgment of the Court of Appeal and remand with instructions to direct the trial court to conduct that inquiry in the first instance. (Cf. *People v. Rodriguez* (2018) 4 Cal.5th 1123, 1132–1133.) On remand, Liu bears the "ultimate burden" of demonstrating, by a preponderance of the evidence, that she

is eligible for Proposition 47 relief. (*Romanowski*, *supra*, 2 Cal.5th at p. 916; Evid. Code, § 115.)

III.

In *Romanowski,* we required a straightforward, if somewhat nuanced, analysis from courts assessing the reasonable and fair market value of stolen access card information. Courts must assess how much such information would sell for, even though it cannot be sold legally. In conducting that inquiry, the value of what a defendant obtained using stolen access card information may be somewhat relevant. But if so, it must be considered along with potentially more probative pieces of the pricing puzzle, such as: (1) the access card's credit limit or the account balance, if knowable when the defendant engages in the acquisition or retention of information that serves as the basis for criminal liability under section 484e(d); (2) the amount of account information possessed by the defendant; (3) how much the value of the information has been diminished because of its sale in illicit markets; (4) how recently the information was stolen; and (5) the prevalence of comparable information on the illicit market.

To allow for the proper valuation in this case, we vacate the judgment of the Court of Appeal and remand with instructions to send the case back to the trial court for further factfinding as to the reasonable and fair market value of the access card information at issue.

CUÉLLAR, J.

We Concur:

CANTIL-SAKAUYE, C. J.
CHIN, J.
CORRIGAN, J.
LIU, J.
KRUGER, J.
GROBAN, J.

See next page for addresses and telephone numbers for counsel who argued in Supreme Court.

Name of Opinion People v. Liu

Unpublished Opinion
Original Appeal
Original Proceeding
Review Granted XXX 21 Cal.App.5th 143
Rehearing Granted

Opinion No. S248130
Date Filed: November 21, 2019

Court: Superior
County: Los Angeles
Judge: Robert P. Applegate

Counsel:

David R. Greifinger, under appointment by the Supreme Court, for Defendant and Appellant.

Xavier Becerra, Attorney General, Gerald A. Engler, Chief Assistant Attorney General, Lance E. Winters, Assistant Attorney General, Steven E. Mercer, Noah P. Hill, and Tita Ngyuen, Deputy Attorneys General, for Plaintiff and Respondent.

Counsel who argued in Supreme Court (not intended for publication with opinion):

David R. Greifinger
Law Offices of David R. Greifinger
15515 West Sunset Boulevard, No. 214
Pacific Palisades, CA 90272
(424) 330-0193

Noah P. Hill
Deputy Attorney General
300 S. Spring Street, Suite 1702
Los Angeles, CA 90013
(213) 269-6082