IN THE COURT OF APPEALS OF THE
STATE OF OREGON

STATE OF OREGON,
*Plaintiff-Respondent,*
*v.*
FINOT TECLE,
*Defendant-Appellant.*
Multnomah County Circuit Court
130431860; A158767

Alicia A. Fuchs, Judge.

Argued and submitted November 15, 2016.

Neil F. Byl, Deputy Public Defender, argued the cause for appellant. With him on the brief was Ernest G. Lannet, Chief Defender, Criminal Appellate Section, Office of Public Defense Services.

Patrick M. Ebbett, Assistant Attorney General, argued the cause for respondent. With him on the brief were Ellen F. Rosenblum, Attorney General, and Benjamin Gutman, Solicitor General.

Before Duncan, Presiding Judge, and DeVore, Judge, and Garrett, Judge.

DEVORE, J.

Convictions on Counts 2, 5, 8, 11, 14, 16, 18, 21, 24, 26, 28, 31, 34, 36, 38, 41, 44, and 47 reversed; Count 10 reversed and remanded for entry of judgment of conviction for identity theft; remanded for resentencing; otherwise affirmed.

**DEVORE, J.**

Defendant appeals a judgment of conviction for 18 counts of identity theft, ORS 165.800; 12 counts of theft in the second degree, ORS 164.045; and 18 counts of computer crime, ORS 164.377(2). He assigns error to the trial court's denial of his motion for a judgment of acquittal on the computer crime counts, arguing that evidence that he knowingly provided false information to banks was not sufficient to show that he "used" a computer within the meaning of ORS 164.377(2), because the state should have been required to prove that he directly accessed or manipulated the banks' computers. After review of the text, context, and legislative history, we agree that the record lacks evidence from which a factfinder could find that defendant "used" a computer or computer system within the meaning of the statute. The trial court, therefore, erred when it denied defendant's motion for a judgment of acquittal on the 18 counts of computer crime. Defendant also assigns error to the trial court's entry of a judgment of conviction on Count 10 for computer crime instead of identity theft. The state concedes the error, and we agree. Accordingly, we reverse defendant's convictions for computer crime, reverse and remand as to Count 10 for entry of a conviction for identity theft, and remand for resentencing.

When denial of a defendant's motion for a judgment of acquittal "centers on the meaning of the statute defining the offense," we review the interpretation of the statute for legal error. *State v. Hunt*, 270 Or App 206, 210, 346 P3d 1285 (2015) (internal quotation marks and citation omitted). In determining the sufficiency of the evidence, we review the facts in the light most favorable to the state to determine whether a rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt. *State v. Cunningham*, 320 Or 47, 63, 880 P2d 431 (1994), *cert den*, 514 US 1005 (1995).

The relevant facts are undisputed. In September and October 2012, defendant engaged in a scheme to defraud two banks. Defendant personally visited several bank branches and opened checking and savings accounts. Defendant provided the banks' employees with false information, primarily

fraudulent social security numbers and home addresses. The bank employees relied on the information defendant provided, entering that information into the banks' computer systems to create bank accounts for defendant. Defendant activated automatic teller machine (ATM) cards and provided worthless checks for deposit into his new accounts. In compliance with federal law, the banks made at least $100 available immediately after defendant opened the accounts, before the checks were processed. Shortly after defendant created the accounts, someone other than defendant used the ATM cards and passwords to withdraw credited funds from the accounts or make purchases before the banks could determine the validity of the checks. As a result, the banks suffered financial losses.

Defendant was charged with multiple counts of identity theft, theft in the second degree, and computer crime. At the close of the state's case, defendant moved for a judgment of acquittal on the computer crime counts, among others, arguing that the state failed to present any evidence that defendant "used" a computer for purposes of ORS 164.377(2). He argued that there was no evidence that he opened an account online or that he withdrew any money from the accounts using an ATM. Defendant argued that, "just because a bank or a business that you go to uses computers, that doesn't mean that [defendant] used a computer." The state countered that defendant was "using a computer system" by "trying to inflate a bank balance" so that money could be withdrawn later from an ATM. In the state's view, providing false information to a bank employee, who then enters that information into the bank's computer database, constitutes "using" a computer under ORS 164.377(2). The trial court denied defendant's motion, and the jury convicted defendant on all counts.

On appeal, defendant renews his arguments made in the trial court. Defendant contends that the state's interpretation of the term "use" under ORS 164.377(2) is overly broad and contrary to the legislature's intent. The state reiterates its arguments, relying primarily on the statute's text and context to contend that defendant "used" the banks' computer systems for purposes of ORS 164.377(2).

The parties' arguments raise a question of statutory interpretation of whether the legislature intended the phrase, to "use" a computer system, to reach defendant's conduct here. In construing a statute, we consider its text, context, and legislative history, to discern legislative intent. *State v. Gaines*, 346 Or 160, 171-72, 206 P3d 1042 (2009).

We begin with the text and context of the computer crime statute.[1] That statute, ORS 164.377(2), provides:

> "Any person commits computer crime who knowingly accesses, attempts to access or uses, or attempts to use, any computer, computer system, computer network or any part thereof for the purpose of:
>
> "(a) Devising or executing any scheme or artifice to defraud;
>
> "(b) Obtaining money, property or services by means of false or fraudulent pretenses, representations or promises; or
>
> "(c) Committing theft, including, but not limited to, theft of proprietary information or theft of an intimate image."

The statute defines various terms, from "access" to "services." For example, to "access" is "to instruct, communicate with, store data in, retrieve data from or *otherwise make use of* any resources of a computer, computer system or computer network." ORS 164.377(1)(a) (emphasis added). The statute, however, does not define its term "use."

Because the legislature has not defined "use," we consider the term's ordinary, plain meaning. *PGE v. Bureau of Labor and Industries*, 317 Or 606, 611, 859 P2d 1143 (1993). The verb "use" at the time the legislature enacted the statute was defined as "to carry out a purpose or action by means of **:** make instrumental to an end or process **:** apply to advantage **:** turn to account[.]" *Webster's Third New Int'l Dictionary* 2524 (unabridged ed 2002). The dictionary explains that "USE is general and indicates any putting

[1] The version of the statute that applies in this case is ORS 164.377 (2011), *amended by* Or Laws 2015, ch 350, § 1, but because the subsequent amendment does not affect our analysis, we cite the current version of the statute throughout this opinion.

to service of a thing, usu[ally] for an intended or fit purpose or person[.]" *Id*. That broad definition of "use" posits a range of meanings, and it begs the question whether to "use" may be directly or indirectly done.

Both parties argue that the text and context of ORS 164.377(2) supports their positions. Defendant observes that the plain meaning of "use" can be either broad or narrow. Defendant argues that the "apply to advantage" definition of "use" connotes a "broad definition in which a person could take advantage of something indirectly, without accessing or manipulating it." Defendant contrasts that meaning of "use" with the meaning of the phrases, "putting to service of a thing" and "mak[ing] instrumental to an end." *Webster's* at 2524. He argues that the latter meaning of "use" connotes a "more narrow definition in which a person directly manipulates something for an intended purpose, and that the thing being used be crucial to achieving that intended purpose." Defendant reasons that, because ORS 164.377(2) requires that the individual "use" the computer "for the purpose of" one of several prohibited activities, the context implies the direct manipulation of the computer for an intended and prohibited purpose, rather than indirectly taking advantage of someone else's manipulation of a computer system. Therefore, defendant posits that the legislature had a narrow definition of "use" in mind—specifically to target computer hackers—when it enacted the computer crime statute.

The state responds that nothing in the statute connotes a requirement that, to "use" a computer in order to execute a fraud, the perpetrator must personally enter the fraudulent information into the computer. Applying one meaning of "use," the state argues that defendant "used" a computer because defendant "carried out his purpose to commit fraud by means of the banks' computer networks." Or, applying another meaning, the state argues that defendant made the banks' computers "instrumental" to the end of committing theft by fraud, and thus "used them for that purpose."

For support, the state cites *State v. Osborne*, 242 Or App 85, 255 P3d 513 (2011) as an application of the dictionary definition of the term "use" in a different statute. In

that case, we concluded that the evidence was sufficient for a jury to find that the defendant "used" a knife for purposes of first-degree robbery, ORS 164.415, when he held a knife in his hand and demanded money from a store clerk. *Id.* at 89-90. *Osborne* does not resolve the question here, however, because, in that case, the defendant personally held the knife to carry out the robbery. Further, dictionary definitions do not resolve our question. "In construing statutes, we do not simply consult dictionaries and interpret words in a vacuum. Dictionaries, after all, do not tell us what words mean, only what words *can* mean, depending on their context and the particular manner in which they are used." *State v. Cloutier*, 351 Or 68, 96, 261 P3d 1234 (2011) (emphasis in original). In this case, further inquiry is needed to determine the legislature's intent.

Like defendant, we acknowledge that the plain meaning of "use" can be broad or narrow. As the parties' textual arguments demonstrate, the court could reach different results depending on how broadly or narrowly the term "use" is construed. Recognizing a similar dilemma in interpreting another subsection of ORS 164.377, the Supreme Court looked to legislative history to understand that subsection based on the "context of the technology of the time." *State v. Nascimento*, 360 Or 28, 42-44, 379 P3d 484 (2016); *see State v. Perry*, 165 Or App 342, 349, 996 P2d 995 (2000), *aff'd*, 336 Or 49, 77 P3d 313 (2003) ("Context may be found in *** the historical context of those relevant enactments."). Although the state's proposed construction of the word "use" in ORS 164.377(2) is plausible, that construction becomes untenable when considered in light of the legislative history.

The statute, ORS 164.377, began as House Bill (HB) 2795. The bill was originally introduced during the 1985 legislative session to combat the theft of cable television services. *See* Bill File, HB 2795 (1985) (before amendment). Representatives of the General Telephone Company urged a House Judiciary subcommittee to adopt an amendment to respond to a related and growing problem at the time, described as "computer crime, or computer hackers if you will." Tape Recording, House Judiciary Committee, Subcommittee 1, HB 2795, May 6, 1985, Tape 576 (statement

of Dave Overstreet, General Telephone Company). Sterling Gibson, an employee of General Telephone Company, explained that many businesses had come to use computers and that the purpose of the amendment was to "prevent people from calling into someone's computer" to manipulate the data and "create havoc to that business or industry." *Id.* (statement of Sterling Gibson). To illustrate the kind of conduct the amendment sought to prohibit, he provided some examples: people who remotely accessed business computers and altered business documents; students who used computers to automatically "scan" telephone exchanges for unsecured computer systems into which they could remotely dial; and individuals who publicly posted confidential long-distance telephone "billing codes" on computer bulletin board systems. *Id.*

That testimony, and other testimony, supports the sense that the bill was targeted at computer hacking and the direct manipulation of information stored within the computer or computer systems. For example, one legislator expressed concern that the amendment might criminalize the conduct of computer hobbyists who used telephone modems of that era to connect with other computers. *Id.* (statement of Rep Kopetski). Marion County District Attorney Dale Penn emphasized that the law would not apply to people who are allowed access to computer systems:

> "There we get into the definition of 'access.' I think *** if you call up to a computer system and you're not authorized you're probably not even going to be able to get the menu up. If you're calling to a bulletin board you're going to see the menu. And that's not what we're addressing here. We're addressing a computer system in which you're not authorized to dial. You won't know the codes."

*Id.* (statement of District Attorney Dale Penn). A committee chair asked why the amendment was necessary in light of a previously enacted "theft of services" statute. Gibson from General Telephone replied that the amendment was concerned with people utilizing computers to "manipulat[e] *** documents that are vital to th[e] organization," which may or may not constitute theft. He stated that, "[a]gain we are not dealing necessarily with the theft of something,

we are dealing with manipulation. We have in the environment computers with the ability of having information being observed by another ***." *Id.* (statement of Sterling Gibson).

The amendments were adopted in the House Judiciary subcommittee and moved to the House Judiciary Committee and the Senate Judiciary Committee, where testimony again focused on computer hacking. At the House Judiciary Committee, legislative counsel stated that the proposed amendment was introduced to address the "idea of *people who use their computers or instruments* to get access to computer systems or networks and then gain by using the information or program that belongs to someone else." Tape Recording, House Judiciary Committee, HB 2795, May 13, 1985, Tape 613, Side A (statement of legislative counsel) (emphasis added). Before the Senate Judiciary Committee, Dave Overstreet, also from General Telephone, emphasized that the "bill address[es] computer hackers—persons who use computers to defraud. Computers can now be used to talk to other computers." Minutes, Senate Judiciary Committee, HB 2795, June 7, 1985, 18 (minutes noting comments; audiotape malfunctioned).

In sum, the legislative history of ORS 164.377 demonstrates that the bill was intended to combat "computer hacking," commonly understood as the practice of gaining access to a computer system and often tampering with sensitive data or information stored within. *See Nascimento*, 360 Or at 42-44. In 1985, the legislature was concerned with people operating a computer to "call[] into someone's computer" to manipulate the data stored within the computer, accessing someone's computer without authorization, and directly using computers for larcenous or fraudulent purposes. There is no indication that the bill was intended to reach the conduct of a person, such as defendant, who simply provided false information to an authorized employee, who then entered that false information into an employer's computer system. The 1985 legislature did not intend to turn ordinary theft or fraud into a computer crime merely when the victim's employee made authorized use of a computer, doing ordinary data entry,

and when the perpetrator did not directly access or manipulate the computer.[2]

The state acknowledges that the legislature's motivation was to criminalize computer hacking, but it argues that the "text the 1985 legislature ultimately adopted is not limited to addressing the problem of trespass-by-computer." The state argues that subsections (3) and (4) criminalize computer use that is "without authorization," so subsection (2) should be construed more broadly to include "areas outside that concern."

In *Nascimento*, 360 Or at 43-44, the Oregon Supreme Court rejected a similar argument about subsection (4) of ORS 164.377. In that case, the issue was the meaning of the phrase, "without authorization." Under 164.377(4), it is a crime to use, access, or attempt to access a computer or computer network "without authorization." ORS 164.377(4).[3] The state urged the court to adopt a broad interpretation of "without authorization," arguing that the defendant's computer use violated her employer's computer use policies and, therefore, her violation of those policies constituted computer crime under ORS 164.377(4).[4] *Nascimento*, 360 Or at 35-36. The court concluded that the legislative history of ORS 164.377 established that the statute was intended to "address the unauthorized access of a computer by 'hackers'

---

[2] We do not address a set of facts in which a bad actor dupes an innocent employee into introducing malicious code or software into an employer's computer system. A violation of ORS 164.377(3) for knowingly and without authorization altering or damaging a computer system does not involve the same term "use." Our decision does not decide such a case. 285 Or App at 393 n 3.

[3] ORS 164.377 provides, in part,

> "(3) Any person who knowingly and without authorization alters, damages or destroys any computer, computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network, commits computer crime.
>
> "(4) Any person who knowingly and without authorization uses, accesses or attempts to access any computer, computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network, commits computer crime."

[4] The defendant in *Nascimento* conceded that she could be convicted under subsection (2) of the computer crime statute for obtaining money by using the computer for false or fraudulent purposes. 360 Or at 35. Regarding subsection (2), the difference in that case is that she had direct access to and manipulation of the lottery terminal.

or others who had no authority to use the computer." *Id.* at 43. The state contended that, even if the legislative history reflected those concerns, "the text that the legislature adopted is 'not so limited,' and that it prohibits *all* 'access' that is 'without authorization.'" *Id.* at 43-44 (emphasis in original). The court rejected the state's interpretation, explaining that the legislature may ultimately choose to adopt "broader language that applies to a wider range of circumstances than the precise problem that triggered legislative attention," but that "does not mean that we necessarily interpret statutes in the broadest possible sense that the text might permit." *Id.* at 44 (internal quotation marks and citation omitted).

Similarly, here, the state urges us to interpret "use" in the broadest possible sense, notwithstanding the narrower legislative history of ORS 164.377. However, we decline to interpret "use" to include the situation in the present case, where defendant did not directly access or manipulate a computer or computer system in the commission of theft or fraud. Although defendant induced the banks to act to permit his theft, at all times the victim banks remained in unqualified and uncompromised control of their computer systems. Therefore, we conclude that defendant did not "use" a computer or computer system within the meaning of ORS 164.377(2). The trial court, therefore, erred in denying defendant's motion for a judgment of acquittal on the computer crime counts.

Defendant also assigns error to the trial court's entry of a judgment of conviction on Count 10 for computer crime instead of identity theft as charged in the indictment and on the verdict form. The state concedes the error. We accept the concession, and remand for entry of a judgment of conviction for identity theft.

Convictions on Counts 2, 5, 8, 11, 14, 16, 18, 21, 24, 26, 28, 31, 34, 36, 38, 41, 44, and 47 reversed; Count 10 reversed and remanded for entry of judgment of conviction for identity theft; remanded for resentencing; otherwise affirmed.