

COURT OF APPEALS OF VIRGINIA

PUBLISHED

Present: Judges Athey, Ortiz and Lorish
Argued at Norfolk, Virginia

TAYLOR AMIL WALLACE

v. Record No. 1040-21-1

COMMONWEALTH OF VIRGINIA

OPINION BY
JUDGE DANIEL E. ORTIZ
FEBRUARY 28, 2023

FROM THE CIRCUIT COURT OF THE CITY OF CHESAPEAKE
John W. Brown, Judge

Samantha Offutt Thames, Senior Assistant Public Defender (Virginia
Indigent Defense Commission, on briefs), for appellant.

Stephen J. Sovinsky, Assistant Attorney General (Jason S. Miyares,
Attorney General, on brief), for appellee.

A person who uses a computer for a fraudulent purpose does not automatically use it “without authority” under the computer fraud statute. Following a bench trial, Taylor Amil Wallace was convicted of computer fraud, obtaining money by false pretenses, uttering forged checks, and failing to appear in court, after she deposited forged checks in an ATM. Wallace challenges the sufficiency of the evidence for each conviction. She argues that the Commonwealth failed to prove that: the ATM is a “computer,” she used the ATM “without authority,” she knew that the checks were forged, and she “willfully” failed to appear in court. We find the evidence insufficient to prove that Wallace used the ATM “without authority” but sufficient to prove the remaining convictions. We affirm in part and reverse in part.

BACKGROUND

In December 2018, Wallace deposited four checks, in the amounts of \$440, \$324, \$450, and \$300, into her bank accounts at BB&T, using a drive-through ATM. These checks were

deposited on four separate days and were made out from Gregory Starling's Southern Bank account to "Taylor A. Wallace." The first two checks had the word "work" in their memo fields, and the third and fourth checks had the words "cleaning" and "remaining balance," respectively. All four checks were endorsed by "Taylor Wallace." Photos from security cameras show Wallace driving to the ATM, sometimes with an unidentified male in the front passenger seat, and depositing the checks. Two of the checks were returned to BB&T as forged. The other two were returned because the Southern Bank account was closed. After using the funds in Wallace's accounts to make up for the loss, BB&T lost \$937.82 in total.

On January 28, 2019, Wallace accepted an interview by Detective Ronald Ward at her mother's residence. Wallace admitted that she was the person depositing the checks and that she did not know Gregory Starling, but she refused to tell Detective Ward where she got the checks. After being arrested and granted bail, Wallace signed a continuance order requiring her to appear before the trial court on January 30, 2020. However, she did not appear on January 30. Wallace was charged with four counts of forging a check, four counts of uttering a forged check, four counts of obtaining money by false pretenses, four counts of computer fraud, one count of using false identification to obtain money, and one count of felony failure to appear, in violation of Code §§ 18.2-152.3, 18.2-172, 18.2-178, 18.2-186.3(A)(2), and 19.2-128(B).

At the bench trial, Wallace testified that she did not steal the checks but received them from her stepfather, Miguel Sumner, who had no bank account and told Wallace that the checks were his paychecks for his demolition and cleaning work. She testified that the unidentified male in the passenger seat was Sumner and that Sumner did not give her the checks until they were at the ATM. She denied having endorsed the checks, claiming that she never actually looked at the checks because she trusted Sumner. Wallace also stated that she had been represented by several attorneys and that, although she signed the continuance order, the advice

from one of her attorneys caused her failure to appear. Wallace was not allowed to testify as to what the attorney told her,¹ and the attorney did not testify at trial. Finally, Wallace stated that she was 18 years old in December 2018 and admitted that she had had one misdemeanor conviction involving lying, cheating, or stealing, as well as three or four felony convictions as a juvenile. Wallace's mother corroborated Wallace's story, testifying that she dated Sumner during the time Wallace deposited the checks and that Sumner worked in construction.

Starling testified that he did not write the four checks and that they were probably taken from his work truck around December 7, 2018. He stated that, at the time, he worked at a job site and had hired a man, James Watson, and an all-male team for demolition and cleaning work.

BB&T investigator Kevin Wolfe testified that the ATM was a "very sophisticated machine" and had "a number of different functions," including depositing checks, withdrawing cash, and making balance inquiries. Wolfe opined that an ATM "would be considered a computer."

After hearing all evidence, the trial court found Wallace guilty of uttering forged checks, obtaining money by false pretenses, computer fraud, and failure to appear. It did not find Wallace guilty of forgery or identity fraud. The trial court sentenced Wallace to 17 years and 96 months of incarceration, with 13 years and 128 months suspended. Wallace appeals, challenging the sufficiency of the evidence for each conviction. First, Wallace argues that the evidence does not support the computer fraud convictions because an ATM is not a computer and Wallace did not use the ATM "without authority." Second, Wallace argues that the evidence does not establish that she possessed the requisite intent for uttering forged checks, obtaining money by

¹ The trial court prohibited Wallace from testifying as to the attorney's advice, finding that such testimony would be inadmissible hearsay.

false pretenses, or computer fraud. Finally, Wallace argues that the evidence did not establish that she “willfully” failed to appear in court.

ANALYSIS

A. Standards of Review

In reviewing the sufficiency of the evidence, we consider the evidence “in the light most favorable to the Commonwealth, the prevailing party below.” *Vay v. Commonwealth*, 67 Va. App. 236, 242 (2017) (quoting *Smallwood v. Commonwealth*, 278 Va. 625, 629 (2009)). In doing so, we “discard the evidence of the accused in conflict with that of the Commonwealth, and regard as true all the credible evidence favorable to the Commonwealth and the inferences to be drawn therefrom.” *Bowman v. Commonwealth*, 290 Va. 492, 494 (2015) (quoting *Kelley v. Commonwealth*, 289 Va. 463, 467-68 (2015)).

We defer “to the trial court’s findings of fact unless they are plainly wrong or without evidence to support them.” *Brewer v. Commonwealth*, 71 Va. App. 585, 591 (2020) (citing *Ramsey v. Commonwealth*, 65 Va. App. 694, 697 (2015)). “The fact finder, who has the opportunity to see and hear the witnesses, has the sole responsibility to determine their credibility, the weight to be given their testimony, and the inferences to be drawn from proven facts.” *Commonwealth v. Taylor*, 256 Va. 514, 518 (1998). Furthermore, “[t]he judgment of a trial court sitting without a jury is entitled to the same weight as a jury verdict” when reviewed on appeal. *Martin v. Commonwealth*, 4 Va. App. 438, 433 (1987) (citing Code § 8.01-680). However, “to the extent that the issue on appeal requires the Court to determine the meaning of a statute and its terms, it reviews that issue *de novo*.” *Brewer*, 71 Va. App. at 591.

B. The evidence is insufficient to establish that Wallace used the ATM “without authority.”

Wallace challenges her computer fraud convictions under Code § 18.2-152.3. She argues that, first, the ATM she used was not a “computer” under the statute, and second, she did not use

the ATM “without authority.” Assuming, without deciding, that the ATM was a computer,² we find that the trial court misinterpreted Code § 18.2-152.3 in finding that Wallace used it “without authority.”

Under the Virginia Computer Crimes Act (“VCCA”), “[a]ny person who uses a computer or computer network, without authority” and “[o]btains property or services by false pretenses,” “[e]mbezzles or commits larceny,” or “[c]onverts the property of another” is guilty of computer fraud. Code § 18.2-152.3. Under the VCCA, “[a] person is ‘without authority’ when he knows or reasonably should know that he has no right, agreement, or permission or acts in a manner knowingly exceeding such right, agreement, or permission.” Code § 18.2-152.2. Wallace argues that as a BB&T customer, she had the authority to use the ATM to deposit checks and withdraw cash. The Commonwealth responds that Wallace exceeded her authority by depositing forged checks. The question here is whether a person who uses a computer to obtain money by false pretenses is per se “without authority.”

“When construing a statute, our primary objective is ‘to ascertain and give effect to legislative intent,’ as expressed by the language used in the statute.” *Cuccinelli v. Rector, Visitors of the Univ. of Va.*, 283 Va. 420, 425 (2012) (quoting *Commonwealth v. Amerson*, 281

² We agree with the dissent that the ATM was a “device that accept[ed] information in digital or similar form and manipulate[d] it for a result based on a sequence of instructions.” Code § 18.2-152.2. However, we decline to find that the ATM fell outside the exception of “specialized computing devices that are preprogrammed to perform a narrow range of functions with minimal end-user or operator intervention and are dedicated to a specific task.” *Id.* The dissent finds that the ATM’s “level of sophistication” was high and that in using the ATM to deposit checks, Wallace was not subject to the “same oversight” of a live-teller transaction. Because Code § 18.2-152.2 does not base the distinction on a machine’s “level of sophistication,” and because the record does not establish how ATM transactions and live-teller transactions are subject to different oversight, we are not ready to reach the same conclusion. Furthermore, we must “decide cases ‘on the best and narrowest grounds available’” under the doctrine of judicial restraint. *Commonwealth v. White*, 293 Va. 411, 419 (2017) (quoting *Commonwealth v. Swann*, 290 Va. 194, 196 (2015)); *see also Spruill v. Garcia*, 298 Va. 120, 127 (2019). Therefore, we decline to reach a finding regarding whether an ATM is a computer under Code § 18.2-152.3.

Va. 414, 418 (2011)). We “presume that the legislature chose, with care, the words it used when it enacted the relevant statute.” *Zinone v. Lee’s Crossing Homeowners Ass’n*, 282 Va. 330, 337 (2011). In addition, “when the General Assembly has used specific language in one instance, but omits that language or uses different language when addressing a similar subject elsewhere in the Code, we must presume that the difference in the choice of language was intentional.” *Id.* Such omission shows “that the General Assembly knows how to include such language in a statute to achieve an intended objective” and unambiguously expressed “a contrary intention.” *Morgan v. Commonwealth*, __ Va. __, __ (Dec. 29, 2022). Finally, when a statute is ambiguous, “the rule of lenity [directs] us to adopt a narrow construction, thus reducing exposure to criminal liability.” *Fitzgerald v. Loudoun Cnty. Sheriff’s Off.*, 289 Va. 499, 508 (2015); *see also Morgan*, __ Va. at __ (applying the rule of lenity when a narrow interpretation of a penal statute did not conflict with legislative intent and was not overly restrictive).

Preventing unauthorized access to computers is a primary purpose of computer crime laws. The federal government and all fifty states have “enacted computer crime laws that prohibit ‘unauthorized access’ to computers.” Orin S. Kerr, *Cybercrime’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes*, 78 N.Y.U.L. Rev. 1596, 1596 (2003); *see also* Susan W. Brenner, *State Cybercrime Legislation in the United States of America: A Survey*, 7 Rich. J.L. & Tech. 28, p15 n.37 (2001) (listing state computer crime statutes). In Virginia, the plain language of the VCCA manifests this legislative intent. The VCCA expressly defines “without authority,” and it is an element of several offenses within the VCCA, including computer fraud. Code §§ 18.2-152.2 and -152.3. The language makes it clear that the computer fraud statute applies only to the *unauthorized* use of computers and computer networks.

Moreover, the words “without authority” clearly modify “use[] [of] a computer or computer network” in Code § 18.2-152.3, rather than the purposes of such use—that is, obtaining property or services by false pretenses, embezzlement, larceny, and conversion. Thus, combining Code §§ 18.2-152.2 and -152.3, a computer fraud conviction requires that the defendant either “has no right, agreement, or permission” to use the computer or computer network or uses it “in a manner knowingly exceeding such right, agreement, or permission.” To prove that a defendant knowingly exceeded their authorization, the Commonwealth must first establish the scope of the right, agreement, or permission. The manner, rather than purpose, of the use must be unauthorized. The dissent argues that our analysis distinguishing the manner and purpose of computer use is “unnecessarily complicated,” but the plain text of the statutes compels such a distinction. The definition of “without authority” explicitly includes “in a *manner* knowingly exceeding” authorization. Code § 18.2-152.2 (emphasis added). At the same time, the words “without authority” in the computer fraud statute do not modify the enumerated purposes of obtaining property by false pretenses, embezzlement, larceny, and conversion.

A comparison of Code § 18.2-152.3 to Code § 18.2-152.5 further supports this conclusion. Under Code § 18.2-152.5, “[a] person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally *examines without authority* any employment, salary, credit or any other financial or identifying information . . . relating to any other person.” (Emphasis added). Unlike in the computer fraud statute, here the words “without authority” modify the *examination* of information, rather than the use of a computer or computer network. For example, in *Ramsey v. Commonwealth*, a state trooper ran inquiries using the Virginia Criminal Information Network (VCIN) for personal purposes, knowing that she was only authorized to do so for criminal justice purposes. 65 Va. App. at 695-96. Although she had authority to use the VCIN, this Court upheld her conviction under

Code § 18.2-152.5 because she “was without authority to examine the information on VCIN for non-criminal justice purposes.” *Id.* at 701. The words “without authority” modify different actions in the computer fraud and computer invasion of privacy statutes. Because both sections of the VCCA address the “similar subject” of computer crimes, “we must presume that the difference in the choice of language was intentional.” *Zinone*, 282 Va. at 337.

We reject the Commonwealth’s argument that if a defendant uses a computer to deposit forged checks—or for unlawful purposes more generally—her use is per se without authority under the computer fraud statute. This interpretation would render the words “without authority” in Code § 18.2-152.3 surplusage. In fact, the General Assembly specifically rejected proposals to remove the words from the statute. *See, e.g.*, Va. St. Crime Comm’n, *Computer Crimes Act*, Rep. Doc. No. 77, at 10 (2005) (recommending eliminating “without authority” from Code § 18.2-152.3 because when “a criminal uses a computer to . . . commit a fraud on another . . . it should not be a possible defense that he had the permission of the owner of the computer to engage in illegal activities”); Senate Bill No. 1163 (Jan. 12, 2005) (amending “[a]ny person who uses a computer or computer network without authority and with intent to” to “[a]ny person who, through the use of a computer”). Moreover, unlike computer fraud, other computer crimes under the VCCA do not include the “without authority” element. *See, e.g.*, Code § 18.2-152.7:1 (harassment by computer); Code § 18.2-152.5:1 (using a computer to gather identifying information). We must presume that the difference in language was intentional.

The unambiguous language of Code § 18.2-152.3 demonstrates that “without authority” modifies the use of the computer itself, rather than the purpose of the use. But even if the language were ambiguous, the rule of lenity would nevertheless compel the same interpretation. If the General Assembly found our traditional fraud statutes insufficient and intended to enhance the punishment for all defendants who use computers or computer networks as a tool in

committing false pretenses, embezzlement, larceny, or conversion, it could have made it clear by eliminating the words “without authority” in the computer fraud statute. Absent such an express legislative intent, we refuse to adopt this broad interpretation.

The Commonwealth argues that a person authorized to use a computer can exceed their authorization, citing *Brewer*, 71 Va. App. at 592, *DiMaio v. Commonwealth*, 272 Va. 504, 507-08 (2006), and *Barnes v. Commonwealth*, No. 2693-98-1, 2000 WL 291436 (Va. Ct. App. Mar. 21, 2000). While the proposition is correct, none of these cases explore the meaning of “without authority.” In *Brewer*, we focused on whether a smartphone constituted a “computer.” 71 Va. App. at 591. In *DiMaio*, the appellant only challenged the sufficiency of the evidence regarding the value of data that he removed from a computer. 272 Va. at 506. Finally, *Barnes* is an unpublished case that does not interpret “without authority.” As such, these cases are of little value in determining the meaning of “without authority.” See *Jones v. Commonwealth*, 293 Va. 29, 50 (2017) (“[S]tare decisis does not ‘foreclose inquiry’ into an issue not previously ‘raised, discussed, or decided.’” (quoting *Chesapeake Hosp. Auth. v. Commonwealth*, 262 Va. 551, 560 (2001))).

While not binding on this Court, well-reasoned opinions from other jurisdictions interpreting similar statutes support our conclusion that “without authority” modifies the *use* of computers and computer networks, rather than the purpose of the use. For example, in *Commonwealth v. Shirley*, 653 S.W.3d 571 (Ky. 2022), the Supreme Court of Kentucky reversed a conviction for unlawful access to a computer when the defendant fraudulently placed barcodes from cheap items onto expensive items and then scanned those barcodes at a Walmart self-checkout register. The court reasoned that the Kentucky statute “[did] not refer to whether the individual is accessing a computer to commit fraud but [did] refer to whether the individual [was] accessing a computer in the way consented to by the owner.” *Id.* at 579. Similarly, in

People v. Golb, 15 N.E.3d 805 (N.Y. 2014), the Court of Appeals of New York vacated a conviction for unauthorized use of a computer when the defendant used a university computer to send emails criminally impersonating others. The court rejected the prosecution’s argument that “using the computer to commit a crime cannot be an authorized use” and found that New York’s computer crime statute was “intended to reach a person who accesses a computer system without permission (i.e., a hacker).” *Id.* at 814. Finally, in *State v. Nascimento*, 379 P.3d 484 (Or. 2016), the Supreme Court of Oregon reversed a defendant’s conviction for computer crimes when she used a lottery terminal to print lottery tickets for herself without paying. The court rejected the “extremely broad definition” that “any time a person uses or accesses a computer for a purpose not permitted by the computer’s owner, the person does so ‘without authorization’ and commits computer crime.” *Id.* at 490. It found that her “use of the lottery terminal to print [lottery] tickets—as she was trained and permitted by her employer to do—was ‘authorized’ use,” despite its ultimately criminal purpose. *Id.* at 491. The purpose of computer crime laws in general, as reflected in these cases, is consistent with our analysis of the VCCA’s language.

Under Code § 18.2-152.3, “without authority” is an element of the crime, for which the Commonwealth has the burden of proof.³ In this case, the Commonwealth presented no evidence to establish the scope of Wallace’s authority to use the ATM or her knowledge that she exceeded such authority. As a bank customer, she had authority to use the ATM to deposit checks and withdraw cash. By depositing a forged check, she used the ATM for an unlawful *purpose*, but not in an unauthorized *manner*. The dissent cites as evidence the facts that BB&T

³ The dissent argues that “[f]or Wallace’s use of the ATM to have been authorized, the evidence would have needed to show that Wallace had BB&T’s permission to use its ATM to perpetrate the fraud that led to her multiple convictions and BB&T’s loss of funds.” This proposition is inconsistent with the general principle that “[t]he Commonwealth has the burden to prove every essential element of the charged crime beyond a reasonable doubt.” *Hubbard v. Commonwealth*, 276 Va. 292, 295 (2008).

investigated the incident, had its representative testify at trial, and was awarded restitution. However, none of these facts establish that Wallace used the ATM in a *manner* knowingly exceeding her authority, and the restitution was based on her fraudulent behavior, not her use of the ATM. Furthermore, the Commonwealth does not cite these facts to show that Wallace used the ATM without authority. Rather, it simply relies on the assumption that any use of a computer or computer network for a fraudulent purpose is per se “without authority.” Because the assumption conflicts with the plain language of Code § 18.2-152.3, we reject it and find the evidence insufficient to establish that Wallace used the ATM “without authority.”

Our interpretation of Code § 18.2-152.3 does not prevent the Commonwealth from obtaining felony uttering convictions in this and similar cases, whereas computer fraud in this case was a Class 1 misdemeanor. Neither does it prevent the Commonwealth from prosecuting, under Code § 18.2-152.3, persons who use their own computers to hack into other computers or computer networks and commit false pretenses, embezzlement, larceny, or conversion. Rather, it simply conforms the scope of Code § 18.2-152.3 to its legislative intent by giving meaning to the words “without authority.”

C. The evidence is sufficient to establish Wallace’s intent to defraud.

Wallace further argues that the evidence is insufficient to establish that she knew the falsity of the checks and that the trial court erred in convicting her of uttering forged checks, obtaining money by false pretenses, and committing computer fraud. To be convicted of uttering forged checks, a defendant must “know it to be forged.” Code § 18.2-172. To be convicted of obtaining money by false pretenses, a defendant must “inten[d] to defraud.” Code § 18.2-178. Finally, a defendant is guilty of computer fraud only when she obtains “property or services by false pretenses,” “[e]mbezzles or commits larceny,” or “[c]onverts the property of another.”

Code § 18.2-152.3. Thus, each conviction required Wallace to know that the checks were forged when she deposited them.

Here, considering all evidence, the trial court was entitled to conclude that Wallace knew the falsity of the checks. Despite Wallace's argument that she was "not a sophisticated banker," the trial court found that Wallace "knew when she got the check that something was wrong." Wallace did not know the payer and was not entitled to be paid, the memo fields reflected work that she did not do, and the checks were already endorsed by someone else in her name. Furthermore, the trial court, as the fact finder, was entitled to find her testimony incredible. Despite Wallace's argument that it was "obvious" that Sumner stole the checks, the trial court refused to "presume" that Sumner was "the thief or that he [was] putting her up to anything, because there is no evidence of that." The trial court concluded that Wallace had "the intent for this scam to succeed" and "did her part." Given the circumstances, the trial court's factual findings were not plainly wrong and should not be disturbed on appeal.

D. The evidence is sufficient to establish that Wallace "willfully" failed to appear in court.

Wallace argues that the evidence is insufficient to establish that she "willfully" failed to appear in court under Code § 19.2-128(B). "Any failure to appear after notice of the appearance date [is] *prima facie* evidence that such failure to appear [was] willful." *Hunter v. Commonwealth*, 15 Va. App. 717, 721 (1993). "When the government proves that an accused received timely notice of when and where to appear for trial and thereafter does not appear on the date or place specified, the fact finder may infer that the failure to appear was willful." *Id.* at 721.

Here, uncontested evidence shows that Wallace signed the continuance order requiring her to appear in court on January 30, 2020, but that she failed to appear on that day. Thus, there is *prima facie* evidence that her failure to appear was willful. While Wallace testified that an

attorney's advice affected her failure to appear, she could not establish what the attorney told her, and the trial court was entitled to determine her credibility as a witness. The trial court "recognize[d] [the] flip-flop in attorneys" but noted that Wallace already had a pending charge of failure to appear and thus "would be on more alert." As such, the trial court's finding that the changes in trial counsel did not overcome the prima facie evidence of willful failure to appear was not plainly wrong.

CONCLUSION

The evidence is insufficient to establish that Wallace used the ATM "without authority" under the computer fraud statute, but sufficient to support the remaining charges. Therefore, we reverse her convictions of computer fraud, affirm her convictions of uttering forged checks, obtaining money by false pretenses, and failure to appear in court, and remand the case for entry of a sentencing order consistent with the rulings of this Court.

Affirmed in part, reversed in part, and remanded.

Athey, J., concurring in part and dissenting in part.

I agree with the majority that the evidence was sufficient to support Wallace's convictions for obtaining money by false pretenses, uttering forged checks, and failing to appear in court. However, I disagree that the evidence was insufficient to establish that Wallace used the ATM without authority. I therefore respectfully dissent from the majority's decision to reverse Wallace's convictions for computer fraud. Since, in my judgment, the evidence sufficiently established that BB&T did not authorize Wallace to use its ATM to obtain money by false pretenses or to utter a forged check, I would have also affirmed Wallace's convictions for computer fraud in violation of Code § 18.2-152.3.

First, the majority "assumes without deciding" that the ATM is a computer. I must therefore briefly explain why I would have decided that this particular ATM meets the definition of a computer pursuant to Code § 18.2-152.2. Initially, Code § 18.2-152.2 broadly defines a "computer" as including "all 'device[s]' not specifically excluded 'that accept[] information in digital or similar form and manipulate[] it for a result based on a sequence of instructions.'" *Brewer v. Commonwealth*, 71 Va. App. 585, 593 (2020) (quoting Code § 18.2-152.2). The computer fraud statute specifically excludes several very basic devices "dedicated to a specific task" requiring "minimal end-user or operator intervention." Code § 18.2-152.2. The limited exceptions include simple calculators, automated typewriters, and fax machines. *Id.* Finally, a "[c]omputer network" means two or more computers connected by a network." *Id.*

Here, the ATM used by Wallace was owned and operated by her local banking institution, BB&T. Wallace was authorized to use the ATM to conduct inquiries as to the balance of her account and to deposit nonfraudulent checks therein. In addition, BB&T account holders, like Wallace, and even clients from other banks were authorized to utilize this ATM to conduct other transactions such as withdrawals. The ATM was also hard-wired to communicate

data transmissions to and from other banks. Moreover, Wallace's authorization to use this "computer" enabled her to utter forged checks more easily since she did not have the same oversight she would have had during a transaction with a live teller.⁴

I would not hold that every ATM should be included within the Code § 18.2-152.2 definition of a computer. For example, some stand-alone ATMs that are solely equipped to dispense cash funds may be more akin to a calculator or fax machine and therefore fall within the statutory exception. However, I would have decided that this particular ATM was clearly a "device that accept[ed] information in digital or similar form and manipulate[d] it for a result based on a sequence of instructions." Code § 18.2-152.2. Since the level of sophistication of this ATM was closer to a computer, I would have rejected Wallace's contention that the ATM was not a computer under Code §§ 18.2-152.2 and 18.2-152.3.

Second, I agree with the majority that "any person who uses a computer or computer network, without authority and . . . [o]btains property or services by false pretenses . . . is guilty of the crime of computer fraud." Code § 18.2-152.3. The majority also correctly states that Code § 18.2-152.3 applies only to the unauthorized use of computers or computer networks. I also agree that "unauthorized" modifies the "use[] [of] a computer or computer network" and that "unauthorized use" means the Commonwealth must prove Wallace either "ha[d] no right, agreement, or permission" to use the computer or computer network or used it "in a manner knowingly exceeding such right, agreement, or permission." However, I simply disagree with the majority's conclusion that since Wallace was authorized to use the ATM for *some* purpose,

⁴ The majority assumes without deciding that this ATM is a computer but, in a footnote, seemingly disagrees with the dissent's conclusion that this ATM meets the definition of a computer pursuant to Code § 18.2-152.2. If the majority contends that this ATM in fact falls within the exception of "specialized computing devices" that are not computers, it should decide the case accordingly since that is a fact-specific inquiry and would indeed be the "narrowest grounds available" on which to decide this case.

she could not exceed that authorization by knowingly using the ATM for an *illegal* purpose—namely, to utter fraudulent checks and thereby obtain money by false pretenses.

By its own definition, the majority contends that “use” becomes unauthorized when someone knowingly exceeds their authority or permission. The majority then engages in an unnecessarily complicated analysis distinguishing the “manner” and “purpose” of such use. In my judgment, the inquiry here is quite simple: Did the Commonwealth prove that Wallace used the ATM in a manner not authorized by BB&T? If the answer is “yes,” the use was unauthorized. If “no,” the use was authorized.

Accordingly, I agree with the Commonwealth’s contention that the computer fraud statute focuses on a defendant’s use of a computer *when the owner does not allow for that kind of use*. In *DiMaio v. Commonwealth*, 46 Va. App. 755, 760 (2005), *aff’d*, 272 Va. 504 (2006),⁵ both this Court and the Supreme Court affirmed an appellant’s computer fraud conviction under Code § 18.2-152.3 when he transferred hundreds of files from his work computer to his personal computer and then deleted the files on his work computer. Admittedly, there, the appellant primarily challenged the sufficiency of the evidence regarding the value of the files he removed from the computer owned by his employer. But nothing in either opinion suggests that because

⁵ I primarily cite *DiMaio* to help illustrate that, under the majority’s theory, situations in which a defendant has permission to use a work computer, friend’s computer, etc. for legitimate purposes (and then exceeds the given authority by engaging in illegal activity) would no longer be subject to prosecution under Code § 18.2-152.3. Essentially, the majority seemingly limits the statute’s application to situations in which a defendant steals a computer or uses one without *any* kind of permission. Since one of the purposes of The Virginia Computer Crimes Act is to enhance penalties for crimes that are less risky to commit, I do not think Code § 18.2-152.3 was meant to be interpreted so narrowly. *See* Va. St. Crime Comm’n, Computer Crimes Act, Rep. Doc. No. 11, at 18 (2005) (noting that “[i]n comparing the risk of computer crimes to that [of] robbery” fewer people will risk committing robbery because “it has a high penalty and is socially unacceptable,” compared to computer crimes where “there are low penalties and in many cases, it is socially tolerable, if not acceptable”).

the appellant had permission to use his work computer, the computer fraud conviction was erroneous because it was not “unauthorized use” under Code § 18.2-152.3.⁶

Simply put, unless Wallace had BB&T’s permission to use the ATM to cash a forged check, keep half of the money, and deposit the other half into her checking account, she used BB&T’s ATM “without authority” pursuant to Code § 18.2-152.3. And although I agree with the majority that Wallace had permission to use the ATM, I disagree that the evidence was insufficient to prove that Wallace “knowingly exceeded” that authority by using the ATM in a manner that BB&T did not and would never authorize. Instead, I would have determined that the evidence sufficiently established that Wallace knowingly exceeded her authority to use BB&T’s ATM. In support thereof, the record reflects that after the checks were flagged, BB&T’s fraud management team investigated the incident and later provided the checks and security camera images of Wallace at the ATM as evidence at trial. In addition, a representative from BB&T assisted the Commonwealth in securing Wallace’s various convictions by testifying on the Commonwealth’s behalf at trial. BB&T was also awarded \$937.82 in restitution. By “regard[ing] as true all the credible evidence favorable to the Commonwealth” and drawing all “fair inferences . . . therefrom,” it seems clear BB&T did not authorize Wallace to use the ATM for fraud. *Vay v. Commonwealth*, 67 Va. App. 236, 242 (2017) (quoting *Parks v. Commonwealth*, 221 Va. 492, 498 (1980)).

⁶ Frequently, when an appellant fails to argue an issue the Supreme Court prefers not to address sua sponte, the Court accepts the concession, but makes clear it is accepting the position because it was conceded, not necessarily because it was legally correct. See e.g., *Daily Press, LLC v. Commonwealth*, ___ Va. ___, ___ (Oct. 20, 2022) (stating that the Supreme Court was not dispositively deciding the conceded issue and “offer[ed] no opinion on” the legitimacy of the conceded standard); *Butcher v. Commonwealth*, 298 Va. 392, 395 (2020) (flagging that although the Supreme Court accepted appellant’s concession that a statute was conjunctive, it “offer[ed] no opinion on the competing conjunctive/disjunctive interpretations of the statute”). In *DiMaio*, neither this Court nor the Supreme Court issued such a disclaimer.

For Wallace's use of the ATM to have been authorized, the evidence would have needed to show that Wallace had BB&T's permission to use its ATM to perpetrate the fraud that led to her multiple convictions and BB&T's loss of funds. I agree with the majority that any fraudulent act committed using another's computer is not per se "without authority."⁷ But I disagree that, based on the unique facts of this particular case, the Commonwealth failed to prove Wallace acted "without authority." Wallace used BB&T's ATM to utter fraudulent checks, and in response to Wallace's use of the ATM, BB&T aided in the fraud investigation, testified at trial with respect to her crimes, produced the fraudulent checks and security camera images used at trial, and is now required to be paid restitution as a result of the fraud.

Since I would have affirmed Wallace's convictions for computer fraud pursuant to Code § 18.2-152.3, I respectfully dissent.

⁷ The majority incorrectly frames the issue as, "whether a person who uses a computer to obtain money by false pretenses is per se 'without authority.'" The answer to that inquiry is clearly "no." Under that interpretation, Code § 18.2-152.3 would criminalize a defendant's use of a co-conspirator's computer. Such a stance would indeed be a misinterpretation of Code § 18.2-152.3. Instead, the issue here is whether there was sufficient evidence to prove that Wallace exceeded her authority to use the ATM when she used it to utter fraudulent checks for payment by BB&T and deposited a portion of the funds from the fraudulent checks in her personal checking account. Considering all the evidence in the light most favorable to the Commonwealth, I simply think there was clearly sufficient evidence to support Wallace's convictions.