COURT OF APPEALS OF VIRGINIA

PUBLISHED

Present: Chief Judge Decker, Judges Humphreys,* Beales, Huff, O'Brien, AtLee, Malveaux, Athey, Fulton, Ortiz, Causey, Friedman, Chaney, Raphael, Lorish, Callins and White
Argued at Richmond, Virginia

TAYLOR AMIL WALLACE

v. Record No. 1040-21-1

COMMONWEALTH OF VIRGINIA

OPINION BY
JUDGE DANIEL E. ORTIZ
JANUARY 23, 2024

UPON A REHEARING EN BANC

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

Samantha Offutt Thames, Senior Appellate Attorney (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. Under the plain text of Code §§ 18.2-152.2 and -152.3, a defendant commits computer fraud only if they "use[]" a computer without permission or "in a manner knowingly exceeding such right, agreement, or permission," not every time they use a computer to commit an enumerated crime. 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. On appeal, Wallace challenged the sufficiency of the evidence for each conviction. A three-judge panel found the evidence sufficient to affirm her convictions on all charges except for four counts of computer fraud. In that regard, the

* Judge Humphreys participated in the hearing and decision of this case prior to the effective date of his retirement on December 31, 2023.

panel found the evidence insufficient to prove that Wallace used the ATM "without authority," with one judge dissenting. Upon the Commonwealth's petition for a rehearing en banc as to the computer fraud charges, this Court finds en banc that the evidence presented at trial failed to prove that Wallace was "without authority" when she accessed her own bank account via an ATM and deposited the checks.

BACKGROUND

On four different days in December 2018, Wallace used a drive-through ATM at BB&T to deposit four checks into her BB&T bank accounts.[1] The checks were made out from Gregory Starling's Southern Bank account to "Taylor A. Wallace." All four checks were endorsed by "Taylor Wallace." Security camera footage shows 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 recouping its losses from Wallace's bank accounts, BB&T suffered a loss of $937.82. In an interview with police officers in January 2019, Wallace admitted that she was the person depositing the checks and that she did not know Gregory Starling, but she refused to say where she got the checks.

At a 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 Sumner was the unidentified male in the passenger seat and that he did not give her the checks until they were at the ATM. She denied having endorsed the checks, claiming that she never looked at the checks because she trusted Sumner. Wallace's mother corroborated Wallace's story, testifying that she

[1] The four checks were for $440, $324, $450, and $300.

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.

At the trial, 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 stated that an ATM "would be considered a computer."

Wallace was convicted of four counts of uttering a forged check, four counts of obtaining money by false pretenses, four counts of computer fraud, and one count of felony failure to appear, in violation of Code §§ 18.2-152.3, 18.2-172, 18.2-178, and 19.2-128(B). The trial court found Wallace not guilty of forgery or identity fraud. *See* Code §§ 18.2-172, -186.3(A)(2). The trial court sentenced Wallace to 17 years and 96 months of incarceration, with 13 years and 128 months suspended.

On appeal, Wallace challenged the sufficiency of the evidence for her convictions for computer fraud, uttering, obtaining money by false pretenses, and failure to appear. As to the computer fraud charges, a three-judge panel held that the evidence was insufficient to show that Wallace acted "without authority," with a single judge in dissent. The panel unanimously upheld her convictions for the other charges. The Commonwealth requested, and this Court granted, a rehearing en banc to reconsider the panel's holding solely related to the computer fraud convictions. Once again, we hold that the trial court erred in determining that Wallace was "without authority" when she used the ATM in question to process the four checks.

Accordingly, we reverse the judgment of the trial court as to Wallace's convictions for computer fraud.

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 all fair 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). "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, 443 (1987). Still, "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. Statutory Interpretation

Wallace challenges her computer fraud convictions under Code § 18.2-152.3. She argues that, first, she did not use the ATM "without authority," and second, the ATM she used was not a

"computer" under the statute. 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 the ATM "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 Va. 414, 418 (2011)). "When the language of a statute is unambiguous, we are bound by the plain meaning of that language." *Id.* (quoting *Kozmina v. Commonwealth*, 281 Va. 347, 349 (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) (quoting *Addison v. Jurgelsky*, 281 Va. 205, 208 (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*, 301 Va. 476, 482 (2022) (quoting *Brown v. Commonwealth*, 284 Va. 538, 545 (2012)). Finally, when a statute is ambiguous, "the rule of lenity [directs] us to adopt a narrow construction, thus

[2] The Commonwealth also argues that Wallace used a computer network as an alternative ground for affirmance. *See* Code § 18.2-152.3 (defining computer fraud as using "a computer or computer network, without authority and" committing a specified theft or fraud crime). Because we find that the Commonwealth failed to prove that Wallace was "without authority," we need not decide whether a computer network was used here. *See Commonwealth v. White*, 293 Va. 411, 419 (2017) (noting that we must "decide cases 'on the best and narrowest grounds available'" under the doctrine of judicial restraint (quoting *Commonwealth v. Swann*, 290 Va. 194, 196 (2015))).

reducing exposure to criminal liability." *Fitzgerald v. Loudoun Cnty. Sheriff's Off.*, 289 Va. 499, 508 (2015).

1. The plain language of Code §§ 18.2-152.2 and -152.3 means that a defendant must "use[]" a computer "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.

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, at 15 n.37 (2001) (listing state computer crime statutes). In Virginia, the plain language of the VCCA expressly defines "without authority" and includes it as an element of several offenses, including computer fraud. Code §§ 18.2-152.2 to -152.3. The language makes it clear that the computer fraud statute applies only to the *unauthorized* use of computers and computer networks.[3]

[3] The dissent suggests that we are unduly reliant upon "factors such as the purpose, reason, and spirit of the law, including any legislative history" in analyzing the statute's meaning. *See Eley v. Commonwealth*, 70 Va. App. 158, 164 (2019). To the contrary, the statute's plain language on its own compels our interpretation of "without authority," while the legislative purpose provides helpful context.

Here, both parties agree that, as a bank customer, Wallace had some "right, agreement, or permission" to use the ATM. *See* Code § 18.2-152.2. At issue is simply whether Wallace "act[ed] in a manner knowingly exceeding such right, agreement, or permission." *See id.* Wallace argues that as a BB&T customer, she had the authority to use the ATM for the functions she performed—depositing checks and withdrawing cash. The Commonwealth responds that while Wallace had authority to use the ATM for lawful purposes, Wallace exceeded her authority by depositing *forged* checks. The question here is whether a person authorized to use a computer necessarily exceeds that authority when they use the computer to obtain money by false pretenses.

In Code § 18.2-152.3, the words "without authority" clearly modify "use[] [of] a computer or computer network," rather than the criminal purposes of such use, enumerated as obtaining property or services by false pretenses, embezzlement, larceny, or conversion. Thus, combining Code §§ 18.2-152.2 and -152.3, a computer fraud conviction requires that a 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 defendant's right, agreement, or permission. The plain text of the statute, which states that a person must act "in a *manner* knowingly exceeding" their authorization, indicates that the manner of use, rather than the purpose of the use, must be unauthorized. Code § 18.2-152.2 (emphasis added). This is distinct from lacking authority to achieve an enumerated purpose of obtaining property by false pretenses, embezzlement, larceny, or conversion. The structure of the statute, pairing "without authority" with "use," rather than the enumerated fraud or theft offenses, tells us that simply committing a listed crime—which is never "authorized," in

the broad legal or moral sense—is not enough to be "without authority." Rather, a person must be "without authority" to use the computer in a certain way.

2. Reading the computer fraud statute in the context of the criminal code clarifies that a person's use, not their purpose, must be "without authority."

A comparison of Code § 18.2-152.3 to Code § 18.2-152.5 also shows that "without authority" relates to an individual's "use." 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*, 65 Va. App. 694 (2015), 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. *Id.* 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. Thus, we must focus on whether a specific "use" of the computer was authorized or not, irrespective of whether the ultimate purpose was lawful.[4]

We reject the Commonwealth's argument that if a defendant uses a computer to deposit forged checks—or for unlawful purposes more generally—their 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. *See Hubbard v. Henrico Ltd. P'ship*, 255 Va. 335, 340 (1998) ("[E]very part of a statute is presumed to have some effect and no part will be considered meaningless unless absolutely necessary."). 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"); S.B. 1163 (as introduced, Jan. 12, 2005) (amending "[a]ny person who uses a computer or computer network without authority and with intent to" to

[4] A similar comparison is possible with Code § 18.2-186.3, criminalizing identity theft, which this Court interpreted recently in *Belcher v. Commonwealth*, 75 Va. App. 505 (2022). Among other things, that section makes it

> unlawful for any person, without the authorization or permission of the person or persons who are the subjects of the identifying information, with the intent to defraud, for his own use or the use of a third person, to: . . . [o]btain money, credit, loans, goods, or services through the use of identifying information of such other person.

Code § 18.2-186.3(A)(2). In the identity theft statute, the "without the authorization" clause modifies the action of obtaining of money or other things of value, not the use of the identifying information. Thus, even if an individual is authorized to use a credit card to buy groceries for their employer, for example, they are not authorized to use that credit card for the purpose of obtaining personal gain by buying groceries for themselves. *See Belcher*, 75 Va. App. at 519-21. The computer fraud statute is structured differently, with the "without authority" clause modifying "use[]," not the ultimate criminal purpose.

"[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 again take the legislature at its word and read "without authority" to require more than commission of an enumerated criminal act.

In support of its broad reading, the Commonwealth relies on several prior cases upholding convictions for computer fraud and related crimes, none of which explore the meaning of "without authority." *See Brewer*, 71 Va. App. at 591-97; *DiMaio v. Commonwealth*, 272 Va. 504, 506-08 (2006); *Barnes v. Commonwealth*, No. 2693-98-1, slip op. at 1-5, 2000 WL 291436, at *1-2 (Va. Ct. App. Mar. 21, 2000). In *Brewer*, we focused on whether a smartphone constituted a "computer." 71 Va. App. at 591. In *DiMaio*, the appellant challenged only 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." *Barnes*, slip op. at 1-5, 2000 WL 291436, at *1-2 (briefly discussing a sufficiency of the evidence claim under Code § 18.2-152.3). 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))).

3. The VCCA definition of "use[]" further clarifies and contextualizes the meaning of "without authority."

Having established that "without authority" modifies the use of the computer, we must also analyze the meaning of "use[]" under the VCCA—another defined term. The VCCA states that "[a] person 'uses' a computer . . . when he attempts to cause or causes a computer . . . to perform or to stop performing computer operations." Code § 18.2-152.2. This definition is mechanical, focused on the user's direct interactions with the computer and the effect of those

interactions on "computer operations," separately defined as "arithmetic, logical, monitoring, storage or retrieval functions and any combination thereof, [which] includes, but is not limited to, communication with, storage of data to, or retrieval of data from any device." *Id.* The statute also clarifies that computer operations include "any function for which that computer was generally designed." *Id.* Thus, to commit computer fraud, a person must "attempt[] to cause" or actually "cause[] a computer" to perform operations—including, but not limited to "arithmetic, logical, monitoring, storage or retrieval functions"—beyond the scope of the functions they are allowed to perform. *Id.* The word "use[]" does not encompass the end goal or purpose of the user, but their specific actions in operating the computer. Those discrete actions must be undertaken "without authority."

4. This Court's reading of the VCCA is supported by persuasive authority from other state courts and the United States Supreme Court, interpreting similar statutes.

While not binding on this Court, well-reasoned opinions from other jurisdictions interpreting similar statutes support our conclusion that "without authority" modifies the manner of 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. *Id.* at 572, 577-79. 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. *Id.* at 810, 814. 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 the defendant's conviction for computer crimes when she used a lottery terminal to print lottery tickets for herself without paying. *Id.* at 485-86. 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. The court found that the defendant's "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, aligns with our analysis of the VCCA's language.

Finally, in *Van Buren v. United States*, 141 S. Ct. 1648 (2021), the United States Supreme Court, interpreting the Federal Computer Fraud and Abuse Act of 1986 ("CFAA"), considered whether a police sergeant violated federal law when, in contravention of department policy, he used a law enforcement license plate database to search for information on an acquaintance's romantic interest in exchange for $5,000. *Id.* at 1652-53. The CFAA penalizes "anyone who 'intentionally accesses a computer without authorization or exceeds authorized access,' and thereby obtains computer information." *Id.* at 1652 (quoting 18 U.S.C. § 1030(a)(2)). Like the VCCA, the CFAA differentiates between those who "intentionally access[] a computer without authorization" and those who "exceed[] authorized access." *See* 18 U.S.C. § 1030(a)(2). The CFAA goes a step further, defining "exceeds authorized access" as "to access a computer with authorization and . . . use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). Dissecting the plain text, with a focus on the word "so," the Court held that to violate the law a

person must access information "that a person is not entitled to obtain by using a computer that he is authorized to access." *Van Buren*, 141 S. Ct. at 1655. The Court concluded that the federal statute did "not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available to them." *Id.* at 1652. This mirrors our conclusion that, under the VCCA, a defendant authorized to use a computer to perform specific tasks is not "without authority," regardless of any "improper motives."[5] *See id.*

In reaching its conclusion, the *Van Buren* Court rejected the Government's position that the CFAA reached any person who was not authorized to obtain information "in the particular manner or circumstances in which he obtained it." *Id.* at 1654 (emphasis omitted). This broader approach would have incorporated access limitations from a laundry list of potential external sources, including "the United States Code, a state statute, a private agreement, or anywhere else," rendering any use of a computer which violated any other legal, moral, or contractual obligation simultaneously a violation of the CFAA. *Id.* at 1655. Similarly, the Commonwealth's approach in this case would mean that any action that simultaneously involved the use of a computer and the commission of a listed fraud or theft crime would be per se "without authority," notwithstanding the General Assembly's express inclusion of that element in Code § 18.2-152.3. Considering the text of the VCCA, we decline to adopt the Commonwealth's reading, which renders the phrase "without authority" superfluous. Rather, we interpret the phrase "right, agreement, or permission" in the context of the term "use[]," defined as the mechanical computer operations performed on the computer, not the user's ultimate ends,

[5] Contrary to the dissent's suggestion, while we find *Van Buren* persuasive in its analysis of a similar statutory scheme, the statutory text, and not federal caselaw, compels our holding.

whether legal or otherwise. *See* Code §§ 18.2-152.2 to -152.3. In sum, though a user's purpose may be illegal, their use may still be authorized.[6]

We note that the VCCA and the CFAA differ in important respects. For example, a person is penalized for unauthorized "access" under the CFAA and "use[]" under the VCCA. *Compare* 18 U.S.C. § 1030(a)(2), (e)(6), *with* Code § 18.2-152.3. "Access" implies the initial approach or entrance to the computer, while "use[]" focuses on the functions or operations performed with the computer. *Compare Van Buren*, 141 S. Ct. at 1657-58, *with* Code § 18.2-152.2. In either case, both statutes require that specific interactions with the computer must be "without authority," not simply the result. The VCCA also lacks the specific word "so" relied upon by the majority in *Van Buren*. *See* 141 S. Ct. at 1655-56. Even so, the framing of the computer fraud definition, in which "without authority" modifies "use[]," and "use[]" means the specific computer operations performed, leads us to the same result as the United States Supreme Court in *Van Buren*.[7]

---

[6] The dissent finds this result strange, suggesting that our reading of the statute eliminates the mens rea requirement in the "without authority" definition. Because we find that Wallace here did not exceed her "right, agreement, or permission" to use the ATM, we may not reach the issue of whether her actions were "knowing" under the statute. *See* Code § 18.2-152.2.

[7] Wallace correctly notes that if Code § 18.2-152.3 were ambiguous, the rule of lenity would compel us to adopt her narrower reading. *See Fitzgerald*, 289 Va. at 508. Nonetheless, because 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, we need not rely on the rule of lenity here. Our narrower interpretation of the statutory language is consistent with the legislative intent of preventing people from using computers without authorization to perpetrate fraud. *See Morgan*, 301 Va. at 483. 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 that 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 Court in *Van Buren* similarly viewed the rule of lenity as "'extra icing on a cake already frosted,'" supporting the conclusion that the statutory term "exceed[ing] authorized access" did not encompass accessing information that the defendant had legitimate authority to

C. Sufficiency of the Evidence

Under Code § 18.2-152.3, "without authority" is an element of the crime of computer fraud, for which the Commonwealth has the burden of proof. 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 perform specific functions on the ATM. She was authorized to use the ATM to deposit checks and withdraw cash—functions "for which th[e ATM] was generally designed." *See* Code § 18.2-152.2. She was similarly authorized to cause the ATM to perform behind-the-scenes storage and retrieval functions to access her account and other accounts. *See id.*

By depositing a forged check, she used the ATM for an unlawful *purpose*, but not in an unauthorized *manner*. The specific computer operations performed—whether viewed as logical, arithmetic, or related to storage and retrieval of data—were the same regardless of the provenance of the checks, whether forged or genuine. Under the statute, then, her use was not "without authority." The Commonwealth's evidence ultimately fails to show that Wallace used the ATM without authority.[8] Rather, the Commonwealth simply relies on the assumption that any use of a computer or computer network for a fraudulent purpose must be "without

---

access, even though the defendant harbored an impermissible purpose. *See Van Buren*, 141 S. Ct. at 1661 (quoting *Yates v. United States*, 574 U.S. 528, 557 (2015) (Kagan, J., dissenting)).

[8] The Commonwealth does point to Starling's testimony that he did not give Wallace permission to use his identifying information or to cash checks written in his name. Here again, we clarify that "without authority" modifies "use[]," which, in turn, modifies the words "computer or computer network." *See* Code § 18.2-152.3. The natural reading of the statute is that only the authorization of the computer owner, not the victim of any related theft or fraud, is required.

authority."[9] Because this assumption conflicts with the plain language of Code § 18.2-152.3, we reject it and find the evidence insufficient to uphold Wallace's convictions.[10]

Our interpretation of Code § 18.2-152.3 does not prevent the Commonwealth from obtaining felony uttering convictions in this and similar cases, though it clarifies and necessarily narrows the application of the computer fraud statute. Nor 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."[11]

---

[9] The Commonwealth correctly notes that "BB&T certainly could not authorize Wallace to violate the law." The dissent also highlights the facts that "after the checks were flagged, BB&T's fraud management team investigated the incidents and later provided the checks and security camera images of Wallace at the ATM as evidence at trial." They also note that a BB&T investigator testified at trial on the Commonwealth's behalf and that BB&T received restitution in the case. Naturally, BB&T did not specifically authorize Wallace to pass bad checks and thereby steal money. BB&T could, however, authorize Wallace to deposit checks and withdraw cash from the bank's own ATM.

[10] We note, as did the Court in *Van Buren*, that based on the record in this case, we need not address whether a person's scope of authority is defined based "only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies." *Van Buren*, 141 S. Ct. at 1659 n.8. Here, no evidence was proffered of any bank policy or customer agreement that specifically barred the use of an ATM to deposit a forged check. As such, we decline to consider what impact, if any, that evidence would have on Wallace's convictions. *See Taylor v. Commonwealth*, 78 Va. App. 147, 157 (2023) (noting that we must decide cases "on the best and narrowest grounds available" (quoting *Swann*, 290 Va. at 196)).

[11] The dissent suggests that this opinion would limit computer fraud convictions to only those cases in which a defendant uses a computer "without *any* kind of permission." Such an interpretation would be at odds with the plain language of the statute, which expressly provides that a person may be "without authority" either when they have "no right, agreement or permission," or when they "knowingly exceed[] such right, agreement or permission." Code § 18.2-152.2. An individual who has authorization to use a friend's computer to complete homework is likely exceeding their authority when they then use the computer to embezzle funds, for example. The distinction lies in looking at whether the specific computer operations performed were authorized. We find that here, Wallace's operations were, in fact, authorized.

CONCLUSION

The evidence is insufficient to establish that Wallace used the ATM "without authority" under the computer fraud statute. Therefore, we reverse her convictions for computer fraud, and remand the case for entry of a sentencing order consistent with the rulings of this Court.

Reversed and remanded.

Callins, J., concurring.

Under the doctrine of judicial restraint, we must decide cases "on the best and narrowest grounds available." *Butcher v. Commonwealth*, 298 Va. 392, 396 (2020) (internal citation omitted). I would decide this case on a crucial threshold question—whether the ATM in question qualifies as a "computer" under Code § 18.2-152.3. Because I would hold that this ATM is *not* a computer, I concur with the majority's decision to reverse and remand Wallace's computer fraud convictions. Resolving this case, however, by determining whether the ATM is a computer would be the best and narrowest grounds available.

Code § 18.2-152.2 defines a "computer" as "a device that accepts information in digital or similar form and manipulates it for a result based on a sequence of instructions." Although "[t]he Act defines the term 'computer' broadly," the definition is not without exceptions. *Brewer v. Commonwealth*, 71 Va. App. 585, 593 (2020). Explicitly excluded are "simple calculators, automated typewriters, [and] facsimile machines." *Id.* at 592 (quoting Code § 18.2-152.2). The statute further excludes as a computer "any other 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.* (quoting Code § 18.2-152.2).[12]

Nothing in the record indicates that the functionality of the subject ATM was more than receiving inputted information and outputting a result, much like a calculator or a facsimile machine. The evidence presented at trial established that, here, the outputted result was

[12] The majority notes that the Commonwealth "argues that Wallace used a computer network as an alternative ground for affirmance." *See* Code § 18.2-152.3 (defining computer fraud as using "a computer or computer network, without authority and" committing a specific theft or fraud crime). It then continues that "we need not decide whether a computer network was used here." I agree. Because I would find that this ATM is not a computer, a computer network is necessarily lacking. *See* Code § 18.2-152.2 (defining a "computer network" as "two or more *computers* connected by a network" (emphasis added)). Thus, there is no need to address whether Wallace used a "computer network" under Code § 18.2-152.3.

extremely limited in scope. Kevin Wolfe, a corporate investigator with BB&T Bank, described the range of functions that the ATM provided: it received deposited checks, expelled cash withdrawals, and displayed balance inquiries.[13] Nothing more. These three functions represent a "narrow range" which the ATM was preprogrammed to accommodate. The record does not indicate *how* this ATM performed these functions, so we have no indication of whether or to what extent information was manipulated as opposed to preprogrammed. *Cf. Midkiff v. Commonwealth*, 54 Va. App. 323, 337 (2009) (describing that in the operation of computer data compilation "how much information will be required about data input and processing to authenticate the output will depend on the nature and completeness of the data, the complexity of the manipulation, and the routineness of the operation" (quoting 2 McCormick on Evidence § 227 (Kenneth S. Broun et al. eds., 6th ed. 2006))). Such evidence would support an inference that this ATM was subject to manipulation and thus was more complex than the devices Code § 18.2-152.2 explicitly excludes.

Accordingly, the ATM in question is comparable to a facsimile machine—a device expressly excluded from Code § 18.2-152.2's definition of a "computer." A facsimile machine receives information inputted by the user. It then transmits that information to another device and confirms the completion of the transmission in the form of an outputted result. A facsimile machine is designed to perform limited functions. This is consistent with the statutory definition of a specialized computing device; it is preprogrammed and dedicated to this specific task.

[13] In determining whether this ATM is a "computer," we consider the evidence introduced at trial. Wolfe testified that this ATM was "a very sophisticated machine that actually has electronics that can actually do a number of different functions." Yet, Wolfe only identified three functions: check depositing, cash withdrawal, and balance inquiry. Notably, Wolfe was not qualified as an expert in ATM machines or in computers. This lack of qualification may account for the conclusory yet dilettante description of "sophisticated machine that actually has electronics" Wolfe provided when asked "what an ATM is." But because neither party challenged Wolfe's qualification to testify on this subject, the above analysis does not take this into consideration.

Likewise, this ATM was preprogrammed and dedicated to its limited range of rudimentary tasks, which Wolfe testified were "depositing checks[,]" "mak[ing] withdrawals[,]" and "balance inquiries."

In conclusion, I would decide this case solely on the issue of whether this ATM is a "computer" under Code § 18.2-152.3. Like my dissenting colleagues, I would not hold that *every* ATM is or is not a computer. Yet, as the evidence here presents nothing more than a machine of limited and preprogrammed functionality, I would hold that the evidence failed to show that this ATM qualified as a computer as defined under Code § 18.2-152.2. Thus, I would reverse and remand Wallace's computer fraud convictions.

Athey, J., with whom Humphreys and Beales, JJ. join, dissenting.

Since Wallace violated Code § 18.2-152.3 when she used the ATM owned by BB&T "without authority" to utter fraudulent checks and thereby obtain money by false pretenses, I would have affirmed Wallace's convictions. Hence, I must respectfully dissent from the majority's decision reversing and remanding her convictions for computer fraud.

Because the majority assumes without deciding that the ATM is a computer, I must first briefly explain why I would have decided that this ATM meets the definition of a computer pursuant to Code § 18.2-152.2. In 2005, the General Assembly broadly redefined the original definition of a "computer" in the Virginia Computer Crimes Act ("VCCA") to include "device[s] 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, 592 (2020) (quoting Code § 18.2-152.2). The new definition excludes several very basic devices "dedicated to a specific task" requiring "minimal end-user or operator intervention." Code § 18.2-152.2 (2005). These excepted devices include simple calculators, automated typewriters, and fax machines. *Id.* Finally, since it's earliest iteration, Code § 18.2-152.2 has defined a computer network as "a set of related, remotely connected devices" that "include[es] more than one computer." Code § 18.2-152.2 (1984).

Here, the ATM used by Wallace was owned by her local banking institution, BB&T. Wallace was authorized to use the ATM to conduct inquiries as to the balance in her account and to deposit nonfraudulent checks therein. In addition, BB&T account holders were authorized to utilize this ATM to conduct other transactions such as withdrawals, transfers, and account inquiries. The ATM was also hard-wired to communicate with BB&T's computer network and to transmit data to and from other banks.

I would not have held that every ATM device should universally fall within the Code § 18.2-152.2 definition of a computer since 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 exceptions. I would, however, have decided that this 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 I would not have found that this ATM was a "specialized computing device[]" only "preprogrammed to perform a narrow range of functions" I would have rejected Wallace's contention that the ATM was excepted from the definition of computer under Code § 18.2-152.2.

In dissenting from the majority's decision reversing and remanding Wallace's convictions for computer fraud, it is worth further explaining the role of the 2005 amendments in modifying the VCCA. The General Assembly modified Code § 18.2-152.3 by removing the requirement that to be found guilty of computer fraud, the Commonwealth must prove that when using a computer without authority, one must do so "with the intent to [o]btain property or services by false pretenses." Code § 18.2-152.3 (1984). Thus, from then on, the Commonwealth must only prove that the computer fraud was committed "without authority." Hence, I agree with the majority that to determine whether Wallace was guilty of computer fraud pursuant to Code § 18.2-152.3, one must first look to the plain meaning of the definitional section of the statute within Code § 18.2-152.2.[14]

In the original 1984 Act, "without authority" was defined as "when [s]he ha[d] no right or permission of the owner to use a computer, or, [s]he use[d] a computer in a manner exceeding

[14] The majority explains in footnote seven that the language in Code § 18.2-152.3 is "unambiguous." I agree, and for this reason would avoid looking to "factors such as the purpose, reason, and spirit of the law, including any legislative history" in analyzing this statute's plain meaning. *See Eley v. Commonwealth*, 70 Va. App. 158, 164 (2019).

such right or permission." Code § 18.2-152.2 (1984). The 2005 amendments further expanded the plain meaning of the term "without authority" by imposing a mens rea element requiring the defendant "know[]" or "reasonably should know" that she was exceeding her permission to use the ATM.[15]

Here, Wallace, a bank customer, was permitted and therefore authorized to use the ATM owned by BB&T. Since Wallace had permission to use the ATM, the only question left to resolve is whether Wallace, by using the computer, acted "in a manner knowingly exceeding such right, agreement or permission." Thus, I would have first held that the ATM unambiguously meets the definition of a computer as defined in the Act. Further, based on the definitions of "use[]" and "without authority," Wallace "use[d]" the "computer" "without authority" because when she used the computer to obtain property by false pretenses, she knowingly acted in a manner exceeding her right or permission to use the ATM owned by BB&T.

The majority incorrectly identifies the issue to be resolved as "whether a person [who is] authorized to use a[n] [ATM] necessarily exceeds that authority when they use the computer to obtain money by false pretenses." The issue is much narrower in that the inquiry is whether, after establishing that the ATM is a computer, the evidence was sufficient to establish that Wallace acted "without authority" because she knew or reasonably should have known "that s[he] ha[d] no right, agreement, or permission" or "knowingly exceed[ed] such right, agreement, or permission."

[15] "Without authority" in its current definition in Code § 18.2-152.2 retains the mens rea component stating that one 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."

Beginning here, I agree with the majority that "without authority" modifies "use[]." "Use[]" as defined in Code § 18.2-152.2 means "when [one] attempts to cause or causes a computer or computer network to perform or to stop performing computer operations." The majority asserts that because "'use[]' does not encompass the end goal or purpose of the user," and instead involves actions taken to operate the computer, Wallace's actions were thus not a "use[]" committed "without authority," and therefore not in violation of the statute.

I disagree with this interpretation and contend that it is clear that the phrase "computer operation" in Code § 18.2-152.2 encompasses various computer "functions" that "include[], but [are] not limited to," the "communication with, storage of data to, or retrieval of data." And further, that a "computer operation" "may also be any function for which that computer was generally designed." Code § 18.2-152.2. The majority's limited definition of computer operations avoids looking at the "function" of the computer here, which was to respond to Wallace's inputs. While I acknowledge that the statutory definition of "use[]" does not speak to the "purposes" or intent of the user, "use[]" *does* encompass the user's "communication with" the machine as well as the "function" that the ATM was designed to serve. For this reason, "use[]" encompasses "computer operation[s]" including "communication[s]" and "function[s]" the ATM was designed to perform like processing checks, and "communicati[ng]" with the computer leading it to perform "any function for which that computer was generally designed." Code § 18.2-152.2.

Thus, based on the plain meaning of Code § 18.2-152.2, "any function for which that computer was generally designed" could be a use pursuant to the statute. "[W]e 'apply[] the plain meaning of the words unless they are ambiguous or [doing so] would lead to an absurd result.'" *Eley v. Commonwealth*, 70 Va. App. 158, 164 (2019) (second and third alterations in original) (quoting *Wright v. Commonwealth*, 278 Va. 754, 759 (2009)). With this principle of

statutory interpretation in mind, I would find that the majority's reliance on *Van Buren v. United States*, 141 S. Ct. 1648 (2021), which interprets a separate federal statute, is misplaced. *Van Buren* involved a police officer's violation of department policy in searching a law enforcement database. *Id.* at 1652-53. Van Buren was prosecuted under 18 U.S.C. § 1030(a)(2) which distinguished between "access[ing] a computer without authorization" and "exceed[ing] authorized access." *Id.* at 1652. 18 U.S.C. § 1030(e)(6) also includes a definitional section which defines "exceeds authorized access" as "access[ing] a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." *Id.*

In *Van Buren*, the United States Supreme Court reversed Van Buren's conviction for computer fraud and found that in order to violate the Computer Fraud and Abuse Act ("CFAA"), an individual must access information "that a person is not entitled to obtain by using a computer that he is authorized to access." *Id.* at 1655. The Court further noted that it would thus not be a violation if a user had "improper motives for obtaining information that is otherwise available to them." *Id.* at 1652. Based on that holding, the majority concludes that *Van Buren* compels this Court to reach the same conclusion here because "a defendant authorized to use a computer to perform specific tasks is not 'without authority.'"

Although the majority acknowledges that the federal statute employs the term "access," but the VCCA employs the term "use[]," the majority avoids acknowledging any meaningful distinction between these disparate state and federal statutes. To illustrate this point, the VCCA defines "use[]" as when a user "attempts to cause or causes a computer or computer network to perform or to stop performing computer operations," Code § 18.2-152.2, while the CFAA fails to define "access." While I agree with the majority that "'[a]ccess' [as used in the CFAA] implies the initial approach or entrance to the computer" and that "'use[]' [as used in the VCCA] focuses

on the functions or operations performed with the computer," it is precisely this distinction that makes the United States Supreme Court's analysis in *Van Buren* irrelevant here.

Similarly, while I agree with the majority that the CFAA does not discuss motive or mens rea for someone who is "access[ing] a computer," I disagree that the VCCA does not contain a reference to "motive." As noted by the majority, the General Assembly chose to retain the term "without authority" when they modified Code § 18.2-152.2 in 2005. However, the 2005 amendments to Code § 18.2-152.2 explicitly added a mens rea component to the definitional section that remains in the current form of the statute in stating "[a] person is 'without authority' when *he knows or reasonably should know* that he has no right, agreement or permission." (Emphasis added).[16] This mens rea requirement concerning the knowledge of the user is directly tied to the user's manner of use, and arguably, this language shows that "without authority" directly contemplates the relevance of the user's purpose. The majority would seem to posit that interpreting "without authority" in a way that assesses the user's intent "relies on the assumption that any use of a computer or computer network for a fraudulent purpose must be 'without authority.'" However, the real issue here, as framed by the Commonwealth, is that Wallace's actions in using a computer "to request funds from the victim's bank or to deposit fraudulent checks" is a use that exceeds the rights and permissions of a bank customer. I thus reject the majority's characterization of the Commonwealth's argument as "if a defendant uses a computer to deposit forged checks . . . their use is per se without authority." And while I would agree that "'use[]' does not encompass the end goal or purpose of the user," I would further conclude that "without authority" does encompass the purposes of the user when she uses a computer.

[16] The 2005 amendments to both Code §§ 18.2-152.2 and -152.3 effectively relocate the "intent" language from the penalty section of Code § 18.2-152.3 to Code § 18.2-152.2 with the addition of the phrase "knows or reasonably should know" to the definition of "without authority."

The penalty section combined with the definition section provide a basis to determine whether a use is "without authority" based on the rights and permissions of a given user in using a computer. As such, it is evident that the circuit court was well within its discretion in finding the evidence sufficient to establish that Wallace's use of the computer in uttering fraudulent checks and thereby obtaining property by false pretenses was committed "without authority," under the circumstances present in this case.[17]

In *DiMaio v. Commonwealth*, 46 Va. App. 755, 760 (2005), *aff'd*, 272 Va. 504 (2006), 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.[18] 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 the appellant had permission to use his work computer, the computer fraud conviction was erroneous because the use was not unauthorized under Code § 18.2-152.3.[19]

---

[17] Based on the same evidence, Wallace was found guilty of uttering under Code § 18.2-172, which contains the requirement that the person "know[s] [the writing] to be forged."

[18] 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 VCCA 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").

[19] Frequently, when an appellant fails to raise an issue, the Supreme Court prefers not to raise the issue sua sponte. The Court usually accepts the concession but makes clear that it is

In *Ramsey v. Commonwealth*, 65 Va. App. 694 (2015), a panel of this Court analyzed a different section of the VCCA specifically involving the "computer invasion of privacy" in which a person is guilty of said offense "when [she] uses a . . . computer network and *intentionally examines without authority* any . . . information . . . relating to any other person." *Id.* at 700. There, we noted that "to be convicted . . . the evidence must establish that the offender viewed identifying information of another 'when [s]he knows or reasonably should know' [s]he is without right, agreement, or permission to do so or 'act[ing] in a manner knowingly exceeding such right, agreement, or permission.'" *Id.* at 698 (third alteration in original). This Court held that "the evidence is sufficient to find appellant was without authority to examine the information on VCIN for non-criminal justice purposes." *Id.* at 701. While the majority distinguishes this result on the basis that "without authority" modified the verb "examine" rather than "use[]," this distinction alone cannot do away with the mens rea component of "without authority" contained in Code § 18.2-152.2 and its relevance to the Court's analysis in *Ramsey*. "Without authority" inherently has an intent element built in, meaning that purpose is as relevant in assessing "use[]" as it was in assessing "examine."

Simply put, unless Wallace had BB&T's permission to use the ATM to cash forged checks, 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. 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 exceed[ed]" that authority by using the ATM in a

---

accepting the position because it was conceded, not necessarily because it was legally correct. *See, e.g.*, *Daily Press, LLC v. Commonwealth*, 301 Va. 384, 411 n.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, 398 (2020) (flagging that although the Supreme Court accepted appellant's concession that a statute was conjunctive, it "[o]ffer[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.

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. The record reflects that after the checks were flagged, BB&T's fraud management team investigated the incidents 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)).

Finding that Wallace's actions in cashing and depositing portions of fraudulent checks in her checking account were done without authority does not make "without authority" superfluous. Instead, this interpretation permits the clear legislative intent of the 2005 General Assembly to be effectuated by allowing courts to determine on a case-by-case basis whether an accused user "knows or reasonably should know" that the use of the computer was committed with "no right, agreement, or permission" or "exceed[s] such . . . permission." The interpretation of the amended Act encouraged by the majority leads to a result that avoids giving any meaning to the terms "knowingly" and "reasonably" inserted by the General Assembly when amending the Act in 2005.[20] For these reasons, I respectfully dissent.

[20] By neutering the requirement that a user "knows" or "reasonably should know" her actions were taken with "no right, agreement, or permission," the strange result is that "though a user's purpose may be illegal, their use may still be authorized."

PUBLISHED

VIRGINIA:

In the Court of Appeals of Virginia on **Tuesday** *the* **28th** *day of* **March, 2023**.

Taylor Amil Wallace, Appellant,

against Record No. 1040-21-1
Circuit Court Nos. CR19-1147-00 through CR19-1147-15 and CR20-649-00

Commonwealth of Virginia, Appellee.

Upon a Petition for Rehearing En Banc

Before Chief Judge Decker, Judges Humphreys, Beales, Huff, O'Brien, AtLee, Malveaux, Athey, Fulton, Ortiz, Causey, Friedman, Chaney, Raphael, Lorish, Callins and White

On March 14, 2023 came the appellee, by the Attorney General of Virginia, and filed a petition requesting that the Court set aside the judgment rendered herein on February 28, 2023, and grant a rehearing *en banc* on the issue(s) raised in the petition.

On consideration whereof and pursuant to Rule 5A:35 of the Rules of the Supreme Court of Virginia, the petition for rehearing *en banc* is granted and the appeal of those issues is reinstated on the docket of this Court. The mandate previously entered herein is stayed pending the decision of the Court *en banc*.

The parties shall file briefs in compliance with the schedule set forth in Rule 5A:35(b). The appellant shall attach as an addendum to the opening brief upon rehearing *en banc* a copy of the opinion previously rendered by the Court in this matter. An electronic version of each brief shall be filed with the Court and served on opposing counsel.[1]

A Copy,

Teste:

A. John Vollino, Clerk

By: *original order signed by a deputy clerk of the Court of Appeals of Virginia at the direction of the Court*

Deputy Clerk

[1] The guidelines for filing electronic briefs and appendices can be found at www.courts.state.va.us/online/vaces/resources/guidelines.pdf.

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.