

**PUBLISHED**

UNITED STATES COURT OF APPEALS  
FOR THE FOURTH CIRCUIT

---

**No. 16-1852**

---

OPENRISK, LLC,

Plaintiff – Appellant,

v.

MICROSTRATEGY SERVICES CORPORATION,

Defendant – Appellee.

---

**No. 16-1906**

---

OPENRISK, LLC,

Plaintiff – Appellant,

v.

MICROSTRATEGY SERVICES CORPORATION,

Defendant – Appellee.

---

Appeals from the United States District Court for the Eastern District of Virginia, at  
Alexandria. Anthony John Trenga, District Judge. (1:15-cv-01451-AJT-TCB)

---

Argued: September 14, 2017

Decided: November 13, 2017

---

Before WYNN, FLOYD, and HARRIS, Circuit Judges.

---

Affirmed by published opinion. Judge Harris wrote the opinion, in which Judge Wynn and Judge Floyd joined.

---

**ARGUED:** Francis Gilbert Gleason, Jr., GLEASON & GLEASON, P.C., Ashland, Massachusetts, for Appellant. Mark Thomas Stancil, ROBBINS, RUSSELL, ENGLERT, ORSECK, UNTEREINER & SAUBER LLP, Washington, D.C., for Appellee. **ON BRIEF:** Kathryn S. Zecca, Donald Burke, Shai D. Bronshtein, ROBBINS, RUSSELL, ENGLERT, ORSECK, UNTEREINER & SAUBER LLP, Washington, D.C., for Appellee.

---

PAMELA HARRIS, Circuit Judge:

In 2011, OpenRisk, LLC contracted with MicroStrategy Services Corporation to create a cloud environment that would host OpenRisk data and programming. But soon after, OpenRisk faced insolvency, and three of its principal officers resigned. At issue in this case is whether MicroStrategy wrongfully continued to provide services to OpenRisk's ex-employees after they had left and formed a new company, Spectant Group LLC.

In particular, OpenRisk alleges that at the direction of its recently departed officers and without its knowledge, MicroStrategy copied and transferred data from the OpenRisk cloud environment to a new environment established for Spectant. And then, according to OpenRisk, MicroStrategy deleted the data from OpenRisk's environment, without the notice of termination required by the parties' contract. When OpenRisk became aware of the copying and deletion of its data, it sued MicroStrategy for computer fraud under Virginia's Computer Crimes Act and for other state-law violations.

The district court granted summary judgment almost entirely in MicroStrategy's favor. The primary issue now on appeal is whether the district court correctly held that the federal Copyright Act preempts OpenRisk's computer fraud claims. We agree with the district court that it does. We further agree that MicroStrategy is entitled to summary judgment on OpenRisk's other claims against it. Accordingly, we affirm the district court's judgment in its entirety.

## I.

### A.

OpenRisk was a start-up company that ceased operations in 2011, shortly after the resignation of three of its key employees: President Craig Ott, Chief Technology Officer Shajy Mathai, and Chief Scientist Richard Murnane. This dispute arises out of MicroStrategy's dealings with the three employees, before and, critically, after their resignations.

Ott, Mathai, and Murnane began their relationship with MicroStrategy even before they formed OpenRisk, using MicroStrategy-licensed software to develop a computer program that would allow insurance companies to analyze exposure to natural disasters. Their business model included the creation of a web-based platform that customers could access on the "cloud," or via the internet. To further this effort, they partnered with investors to establish OpenRisk in January 2011, and in September 2011, OpenRisk contracted with MicroStrategy for "cloud services."

Under the parties' contract, MicroStrategy agreed to provide OpenRisk with access to space on MicroStrategy's servers – a "cloud environment" – on which OpenRisk would store data and run the software it was licensing. In exchange, OpenRisk agreed to make initial payments to MicroStrategy of \$15,000 on October 31 and November 30, 2011, followed by quarterly payments of \$63,000 thereafter, totaling approximately \$1.26 million over the contract's five-year term.

But at the time it entered into this contract with MicroStrategy, OpenRisk was already in dire financial straits. When OpenRisk was unable to close negotiations with a

new investor, Ott, Mathai, and Murnane all resigned from OpenRisk and formed a new company, Spectant. And with MicroStrategy's help, OpenRisk alleges, they took OpenRisk's data with them.

Specifically, OpenRisk points in its complaint to two key acts by MicroStrategy. First, on December 13, 2011, just hours after receiving a cease-and-desist letter from OpenRisk urging it to "cease and refrain from doing any work and making any efforts to commercialize the OpenRisk property with [Ott, Mathai, and Murnane]," J.A. 1068–70, MicroStrategy copied the data from the OpenRisk cloud environment and transferred it to a new environment created for Spectant. And second, on or around January 11, 2012, and after OpenRisk failed to make its first quarterly payment under the contract, MicroStrategy deleted the entire OpenRisk environment and all of its contents from its servers. Only after the data had been erased, on January 20, 2012, did MicroStrategy provide OpenRisk with notice of contract termination for non-payment.

## **B.**

OpenRisk sued MicroStrategy in the United States District Court for the Eastern District of Virginia, invoking the court's diversity jurisdiction. With respect to MicroStrategy's transfer of computer data from the OpenRisk to the Spectant cloud environment, OpenRisk raised Virginia state-law claims of conversion of intellectual property; computer fraud by embezzlement, larceny, and conversion under the Virginia Computer Crimes Act ("VCCA"); and misappropriation of trade secrets. The deletion of data from the OpenRisk environment, OpenRisk alleged, constituted unlawful trespass under the VCCA. OpenRisk also claimed that MicroStrategy tortiously interfered with

the post-employment contractual duties owed to OpenRisk by its former employees, and engaged in unlawful business and civil conspiracies under Virginia law.<sup>1</sup>

At the close of discovery, MicroStrategy moved for summary judgment, arguing that the federal Copyright Act preempts OpenRisk's state-law claims for conversion and computer fraud, and that OpenRisk had failed to put forward sufficient evidence to support a favorable verdict on its other claims. OpenRisk cross-moved for partial summary judgment on its computer fraud and trespass claims under the VCCA. The district court ruled for MicroStrategy, denying OpenRisk's motion and granting MicroStrategy's motion for summary judgment on all claims relevant here.<sup>2</sup>

The court began with what is now the primary issue on appeal: whether state-law claims arising from the copying and transfer of OpenRisk's computer data are preempted by the federal Copyright Act. The district court held that they are. In "substance," the district court explained, OpenRisk's claims for conversion and, under the VCCA, for embezzlement and larceny, all are premised on "underlying conduct" that falls within the scope of copyright protection – the unauthorized copying of data – and thus preempted. J.A. 527. As for the deletion of data from the OpenRisk environment, the court held, OpenRisk could not prevail on its claim of trespass under the VCCA because it had failed

---

<sup>1</sup> Under the express terms of the contract, the parties' dispute is governed by Virginia law.

<sup>2</sup> The district court denied summary judgment on OpenRisk's claim for misappropriation of trade secrets, though it was skeptical that the claim ultimately could succeed. Before OpenRisk filed its notice of appeal, the parties stipulated to dismissal of that claim with prejudice.

to create a genuine issue of material fact as to whether it had sustained the requisite injury as a result of MicroStrategy's conduct. The court also noted a "substantial" threshold question as to whether the deletion of data governed by a contract "even falls within the scope" of the VCCA – a criminal statute – rather than giving rise to an ordinary breach of contract action. J.A. 528.

With respect to OpenRisk's claim for tortious interference, the district court held that OpenRisk had "not come forward with evidence that would allow a reasonable fact finder to conclude" that MicroStrategy had induced or caused OpenRisk's former officers to violate any contractual obligations they may have owed to OpenRisk. J.A. 526. On the contrary: "The evidence . . . quite clearly shows that these officers, independent of any interaction with MicroStrategy . . . had decided to leave OpenRisk and embark upon the efforts they made to operate and create Spectant." *Id.* Finally, the court granted summary judgment to MicroStrategy on OpenRisk's conspiracy claims, finding that OpenRisk had failed to introduce sufficient evidence that the defendants had "engaged in an agreement with anyone" to harm OpenRisk. J.A. 529. And in any event, the court concluded, because the conspiracy claims were predicated on allegations of conversion, larceny, and embezzlement that were themselves preempted, neither could go forward as a matter of law.

OpenRisk filed a motion for reconsideration, which the district court summarily denied. OpenRisk then filed two notices of appeal, and the appeals were consolidated before this court. *See Thomas v. Ford Motor Co.*, 244 F. App'x 535, 538 n.2 (4th Cir. 2007); *see also* Fed. R. App. P. 4(a)(2).

## II.

### A.

OpenRisk’s first argument on appeal is that the district court erred in holding that its computer fraud claims under the VCCA are preempted by the federal Copyright Act. We review the district court’s preemption determination de novo, *Walker v. Medtronic, Inc.*, 670 F.3d 569, 577 (4th Cir. 2012), and come to the same result. As the district court concluded, OpenRisk’s computer fraud claims are preempted because, at their “core,” they seek to impose liability for the unauthorized copying and distribution of data on OpenRisk’s cloud environment, and thus are not “qualitatively different” from copyright infringement claims. *See Rosciszewski v. Arete Assocs.*, 1 F.3d 225, 230 (4th Cir. 1993).

Federal Copyright Act preemption is “broad and absolute.” *United States ex rel. Berge v. Bd. of Trs.*, 104 F.3d 1453, 1464 (4th Cir. 1997). Under § 301 of the Copyright Act,

all legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright . . . and come within the subject matter of copyright as specified by sections 102 and 103 . . . are governed exclusively by this title. . . . [N]o person is entitled to any such right or equivalent right in any such work under the common law or statutes of any State.

17 U.S.C. § 301(a). Congress precluded state-law actions to enforce rights protected by federal copyright law in “the clearest and most unequivocal language possible,” so as to “avoid the development of any vague borderline areas between State and Federal protection.” *Berge*, 104 F.3d at 1464 (quoting H.R. Rep. No. 94-1476, at 130 (1976)). Where Congress has struck the balance between the free flow of ideas in the public



domain, on the one hand, and the protection of certain forms of intellectual property, on the other, § 301 ensures that states may not upset that balance by offering protection that the Copyright Act does not. *See id.* at 1464–65; *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1453 (7th Cir. 1996).

Section 301 thus “sets up a two-prong inquiry to determine when a state law claim is preempted.” *Berge*, 104 F.3d at 1463. First, the work at issue – in this case, software and data from the OpenRisk cloud environment – “must be within the scope of the subject-matter of copyright as specified in 17 U.S.C. §§ 102, 103.” *Id.* If it is, then a state-law claim is preempted if “the rights granted under state law” are “equivalent to” those protected by federal copyright. *Id.* (internal quotation marks omitted). Here, there is no question as to the first prong; OpenRisk does not dispute that the materials in question fall within the scope of the subject matter of copyright. *See, e.g., Trandes Corp. v. Guy F. Atkinson Co.*, 996 F.2d 655, 659 (4th Cir. 1993) (explaining that a “computer program . . . clearly comes within the ‘subject matter’ of copyright”). Accordingly, this case turns on the second prong of the inquiry, and whether the rights OpenRisk seeks to protect under state law are “equivalent to the exclusive rights reserved to the owner of a copyright.” *Id.* at 659.

Chief among those federal-law “exclusive rights” are the rights “to reproduce” and to “distribute copies . . . of the copyrighted work.” 17 U.S.C. § 106(1), (3). So to the extent that OpenRisk’s state claims turn on an allegation that MicroStrategy made unauthorized copies of the data on the OpenRisk cloud environment and then transferred that data to Spectant, those claims are precisely “equivalent” to copyright law’s

prohibition of unauthorized reproduction and dissemination, and hence preempted. As we have held, when the “core” of a state claim is the unauthorized copying of a computer program, the federal Copyright Act precludes that claim from going forward. *See Rosciszewski*, 1 F.3d at 230.

That general principle is readily applied to OpenRisk’s conversion claim – and, indeed, OpenRisk no longer disputes that this claim is preempted. Under Virginia law, “[c]onversion is the wrongful assumption or exercise of the right of ownership over goods or chattels belonging to another in denial of or inconsistent with the owner’s rights,” *Maine v. Adams*, 672 S.E.2d 862, 869 (Va. 2009) (internal quotation marks omitted) – essentially, converting another’s property to one’s own use. And it is clear that when a conversion claim – like OpenRisk’s – rests on an allegation of wrongful copying and distribution of intellectual property, it is “equivalent” to a copyright infringement claim and thus preempted under the Copyright Act. “[W]here the core of the state law theory of recovery, as in conversion, goes to wrongful copying . . . it is preempted.” *Berge*, 104 F.3d at 1464; *see* J.A. 525 (finding it “clear,” based on *Berge*, that OpenRisk’s conversion claim is preempted).

Like the district court, we conclude that OpenRisk’s VCCA computer fraud claims fare no better. The VCCA, a criminal statute with a private right of action, provides in relevant part that “[a]ny person who uses a computer or computer network, without authority and . . . [e]mbezzles or commits larceny . . . is guilty of the crime of computer fraud.” Va. Code Ann. § 18.2-152.3(2). We have held already, reviewing an earlier iteration of the VCCA, that when a claim is predicated on the copying of computer data,

the statutory requirement of “use of a computer” does not “qualitatively change the nature” of the claim so that it is no longer preempted, because “use of the computer ‘is a necessary condition to [the] copying.’” *Rosciszewski*, 1 F.3d at 230 (quoting 1 Melville B. Nimmer & David Nimmer, *Nimmer on Copyright* § 1.01[B], at 1-14 n.62 (1992)). So too for the requirement that the copying be done “without authority,” which also is a necessary condition to copyright infringement. *Id.*

OpenRisk argues, however, that the VCCA’s predicate acts of embezzlement and larceny are different, in that both contain “extra element[s]” that distinguish VCCA computer fraud claims from a copyright infringement claim. And, indeed, when a state-law claim requires an “extra element” – an element that goes beyond the elements of copyright infringement, such as unauthorized reproduction or distribution – that claim may be saved from Copyright Act preemption. *See Berge*, 104 F.3d at 1463 (quoting *Rosciszewski*, 1 F.3d at 229–30). But, critically, not any “extra element” will do. Only when an extra element “changes the nature of the action so that it is ‘*qualitatively* different from a copyright infringement claim’” is preemption avoided. *Id.* at 1463 (quoting *Rosciszewski*, 1 F.3d at 229–30); *see also, e.g., Tire Eng’g & Distrib., LLC v. Shandong Linglong Rubber Co.*, 682 F.3d 292, 311 (4th Cir. 2012) (“A state cause of action is not ‘equivalent’ and avoids preemption if the action requires an ‘extra element [that] *transform[s] the nature of the action . . .*’”) (quoting *Laws v. Sony Music Entm’t Inc.*, 448 F.3d 1134, 1144 (9th Cir. 2006)) (emphasis added).

Applying this standard, we have held that a state action for copying of computer data is preempted by the Copyright Act notwithstanding an “extra element” requiring

“awareness or intent.” *Rosciszewski*, 1 F.3d at 230 (quoting *Computer Assocs. Int’l, Inc. v. Altai, Inc.*, 982 F.2d 693, 717 (2d Cir. 1992)). An intent element, we explained, does not “qualitatively chang[e] a state claim from one of unauthorized copying.” *Id.* It may alter the “scope” of the state claim as compared to a federal copyright action, but it does not affect the underlying “nature” of the claim itself. *Id.* (quoting *Computer Assocs. Int’l*, 982 F.2d at 717). On the other hand, in yet another case involving alleged improper acquisition of computer software, we held that a state claim for trade secret misappropriation is *not* preempted when an “extra element” requires “the breach of a duty of trust or confidentiality.” *Trandes Corp.*, 996 F.2d at 660. Because that element – “the employment of improper means to procure the trade secret, rather than mere copying or use” – is the “core” of a trade secret misappropriation claim, we concluded, it “qualitatively distinguishes such trade secret causes of actions from claims for copyright infringement.” *Id.* (internal quotation marks omitted).

OpenRisk’s primary argument is that the VCCA predicate act of embezzlement includes an additional element that transforms the “nature” of its claim, see *Rosciszewski*, 1 F.3d at 230, bringing it within the rule of *Trandes Corp.* According to OpenRisk, embezzlement under Virginia law requires a showing that a defendant was “entrusted” with property that he or she then wrongfully appropriated, and that extra element of “entrustment” – much like the element of “duty of trust or confidentiality” at issue in *Trandes Corp.* – is enough to save its claim from Copyright Act preemption. We disagree.

The problem with OpenRisk’s argument is its premise: In fact, an embezzlement claim under Virginia law does not include as an “extra element” a special relationship of trust or confidence that might qualitatively distinguish it from a claim for copyright infringement. Our preemption analysis focuses on “the elements” of a state cause of action and not “the facts pled to prove” it, *Trandes Corp.*, 996 F.2d at 659, so regardless of whether OpenRisk has alleged in this case that MicroStrategy abused a trust relationship, what matters are the necessary elements of embezzlement. And as we have explained, the “traditional concept” of embezzlement includes both the “central element” of the “conversion of property belonging to another” and also the “further element[]” that the “property must have been in the lawful possession of the defendant at the time of its appropriation.” *United States v. Stockton*, 788 F.2d 210, 216–17 (4th Cir. 1986). There is no additional requirement – let alone an element at the “core” of the action, *Trandes Corp.*, 996 F.2d at 660 – that the defendant abuse a confidence in the course of committing the crime. *Stockton*, 788 F.2d at 216–17.<sup>3</sup>

Virginia’s embezzlement statute tracks this “traditional concept.” It does reach, as OpenRisk urges, the theft of property that has been “entrusted” to a defendant and is thus within his or her lawful possession. Va. Code Ann. § 18.2-111. But it also reaches the

---

<sup>3</sup> The final element of the traditional crime of embezzlement is that a defendant act with knowledge that his appropriation of property is unauthorized. *Stockton*, 788 F.2d at 217. But as noted above, for Copyright Act preemption purposes, a knowledge or intent element “alter[s] [an] action’s scope but not its nature,” and will not save from preemption a claim otherwise resting on wrongful copying or distribution. *Rosciszewski*, 1 F.3d at 230 (quoting *Computer Assocs. Int’l*, 982 F.2d at 717).

theft of property that has been “*delivered to* [a defendant] by another or by any court, corporation or company,” and has come within the defendant’s lawful possession by this alternative means. *Id.* (emphasis added). And, as the Virginia courts have made clear, “the existence of a formal fiduciary relationship is not necessary” for liability. *Chiang v. Commonwealth*, 365 S.E.2d 778, 780 (Va. Ct. App. 1988).

This understanding of the elements of embezzlement is confirmed by the Supreme Court of Virginia’s decision in *Stegall v. Commonwealth*, holding that a defendant may be guilty of embezzlement for failing to return a rental car. 160 S.E.2d 566, 569 (Va. 1968). A customer has no special relationship of trust or confidence with a car-rental company. Nevertheless, the court found it sufficient that the defendant was “entrusted” with the car, in the sense that he “came into lawful possession of [it] through a rental agreement.” *Id.* at 568–69. OpenRisk does not contend that an element of lawful possession, by itself, would qualitatively distinguish its embezzlement claim from a copyright infringement claim. *Cf. Berge*, 104 F.3d at 1463 (element requiring unlawful possession affects scope but not nature of copying claim). Nor does OpenRisk take the position that a contractual agreement like the one in *Stegall* is an element of Virginia embezzlement law, or that, if it were, it would change the “core” of an embezzlement action so as to save it from Copyright Act preemption. We think this is wise. Agreements not to misuse copyrighted materials are a routine feature of the digital age – every song purchase on iTunes is accompanied by an electronic promise not to violate the exclusive rights set out in the Copyright Act – and if state-law actions to vindicate those agreements were deemed qualitatively different from copyright infringement claims,

there would be little left of Copyright Act preemption. *See* 1 Melville B. Nimmer & David Nimmer, *Nimmer on Copyright* § 1.01[B][1][a][iii] (2017) (state-law claim for violation of “shrinkwrap license” agreement is attempt to “vindicate rights indistinguishable from those accorded by the Copyright Act” and thus preempted).

In sum, embezzlement as defined by Virginia law does not include an “extra element” that makes OpenRisk’s embezzlement claim “qualitatively different” from one for copyright infringement. *See Berge*, 104 F.3d at 1463. As the district court explained, the “substance” of OpenRisk’s embezzlement claim is based on the “same underlying conduct” – the unauthorized copying and transfer of material from the OpenRisk cloud environment – that would support a copyright infringement claim. J.A. 527. Any additional element required to prove state-law embezzlement “relates to the scope” of that action, *id.*, and not to its “nature.” *Rosciszewski*, 1 F.3d at 230.

Application of the “extra element” standard to OpenRisk’s larceny theory is even more straightforward, and leads to the same result. Under Virginia law, larceny is the “wrongful or fraudulent taking of personal goods . . . , belonging to another, without his assent, and with the intention to deprive the owner thereof permanently.” *Foster v. Commonwealth*, 606 S.E.2d 518, 519 (Va. Ct. App. 2004) (quoting *Dunlavey v. Commonwealth*, 35 S.E.2d 763, 764 (Va. 1945)). OpenRisk contends that a VCCA claim predicated on larceny is qualitatively different from copyright infringement because it involves the taking of property without the owner’s consent. But a copyright claim, too, necessarily involves unauthorized reproduction, so this “extra element” is not “extra” at all. *See Rosciszewski*, 1 F.3d at 230 (requirement that computer be used “without

authority” to copy programming does not distinguish computer fraud claim from copyright infringement claim, which “necessarily involves using the computer without authority”). The core of OpenRisk’s claim remains the unauthorized copying and transfer of its data, and that claim is “equivalent to” a copyright infringement action and thus preempted.

## B.

OpenRisk next challenges the district court’s grant of summary judgment to MicroStrategy on its computer trespass, tortious interference, and conspiracy claims. Summary judgment is appropriate when there are no genuine issues of material fact and the moving party – here, MicroStrategy – is entitled to judgment as a matter of law. *Hoschar v. Appalachian Power Co.*, 739 F.3d 163, 169 (4th Cir. 2014). To defeat summary judgment, the non-moving party, OpenRisk, must “provide more than a scintilla of evidence – and not merely conclusory allegations or speculation – upon which a jury could properly find in its favor.” *Design Res., Inc. v. Leather Indus. of Am.*, 789 F.3d 495, 500 (4th Cir. 2015) (internal quotation marks omitted). We review the district court’s award of summary judgment de novo, viewing the evidence in the light most favorable to OpenRisk. *Id.*

First, OpenRisk alleges that MicroStrategy violated the VCCA’s computer trespass provision, Va. Code Ann. § 18.2-152.4(A)(3), by deleting or altering the data on the OpenRisk cloud environment in January 2012, when OpenRisk failed to make the first quarterly payment on its contract. Not until after taking down the cloud environment, OpenRisk claims, did MicroStrategy provide it with the 90-day notice of



termination for non-payment mandated by the parties' contract. Under the VCCA, only a party who is "injured by reason of a violation" of the computer trespass provision may bring a private right of action, *id.* § 18.2-152.12(A), and the district court held that OpenRisk had failed to come forward with the necessary evidence of injury. We agree.

As the district court explained, by the time MicroStrategy stopped maintaining the OpenRisk cloud environment on its servers in January 2012, effectively erasing the contents, "OpenRisk by its own declaration was out of business." J.A. 528. And indeed, as early as November 2011, OpenRisk's CEO informed MicroStrategy that OpenRisk would be "closing company operations" and that MicroStrategy should "discontinue all services to OpenRisk." J.A. 759. But as the district court emphasized, OpenRisk did not request that MicroStrategy preserve or return the information in question. "There's no evidence that the information was needed by OpenRisk for any particular purpose or that MicroStrategy was told [OpenRisk] needed it for any particular purpose." J.A. 528.

OpenRisk argues that the district erred by adopting a *per se* rule that once a company goes out of business, it cannot be injured by the destruction of its property. According to OpenRisk, that rule fails to account for the decrease in OpenRisk's liquidation value that would have resulted from the loss of the material on its cloud environment. But the district court did not announce the *per se* rule imagined by OpenRisk; instead, it made a fact-specific determination that in this case, OpenRisk had proffered no evidence that it had any need or use for the data in question at the time it was deleted. We agree with that assessment of the record. OpenRisk's conclusory assertion that its liquidation value would have been affected negatively by

MicroStrategy's actions is just that – a conclusory assertion without support in the record, insufficient to defeat summary judgment. *See Design Res., Inc.*, 789 F.3d at 500 (party opposing summary judgment must point to more than “conclusory allegations or speculation”).

Like the district court, J.A. 528, we also think that a “substantial” threshold issue would be raised by application of the VCCA’s criminal trespass provision to what appears to be a garden variety breach-of-contract claim. Much of OpenRisk’s argument is directed to a contract provision that expressly allowed MicroStrategy to “irretrievably delete” the metadata on the OpenRisk cloud environment 90 days after notice of termination of the parties’ contract, J.A. 1236, and to whether MicroStrategy complied with that provision when it deleted *all* of the OpenRisk content *before* sending a formal notice of termination. But failure to comply with the terms of a business contract generally is the stuff of civil suits for breach of contract, not criminal liability. And one Virginia court already has held that the VCCA’s computer trespass provision does not apply to a dispute between two parties to a business contract – a service provider and a customer – over deletion of data relating to the customer’s site from the provider’s servers: “[T]his is a question of breach of contract rather than criminal trespass. The contract allowed [defendant AOL] access that might otherwise have been trespass. If the access involved actions that violated the contract, then [p]laintiff can recover for breach of contract.” *CigarCafe, L.C. v. Am. Online, Inc.*, 50 Va. Cir. 146, 157 (Va. Cir. Ct. 1999). But like the district court, we may leave this question of state law for another day. Because OpenRisk failed to come forward with evidence of injury, the district court

properly granted summary judgment to MicroStrategy on OpenRisk’s computer trespass claim.<sup>4</sup>

OpenRisk’s next claim is for tortious interference with contract, alleging that MicroStrategy improperly interfered with post-employment contractual duties owed to OpenRisk by its former officers. Those duties, OpenRisk alleges, included the “non-use” of OpenRisk property, and MicroStrategy made such use possible by transferring OpenRisk data to a cloud environment it had established for Spectant. The district court granted summary judgment to MicroStrategy, holding that OpenRisk had not “come forward with evidence that would allow a reasonable fact finder to conclude that [this] conduct on the part of [MicroStrategy] induced the former officers” to violate any contractual duty. J.A. 526. Again, we agree.

The district court “reviewed the evidence in the case” and determined that it showed, “quite clearly,” that OpenRisk’s ex-employees made an “independent” decision to use “whatever intellectual property OpenRisk may have had” when they established their new company, Spectant. J.A. 526. And as the district court held, that is enough to defeat a claim of tortious interference under Virginia law, which requires evidence that a

---

<sup>4</sup> Tracking the terms of the VCCA’s computer trespass provision, which makes it a crime to “[a]lter, disable, or erase any computer data,” Va. Code Ann. § 18.2-152.4(A)(3), OpenRisk framed its computer trespass claim in terms of deletion and alteration. It now suggests that the district court erred by addressing only its deletion claim and not a separate claim for alteration. But the parties, like the VCCA, regularly treated the two theories together as one claim, and the better reading of the district court’s oral ruling is that “deletion” was used as a shorthand to cover both. In any event, because OpenRisk has failed to provide evidence of injury resulting from MicroStrategy’s decision to cease maintaining OpenRisk’s cloud environment, it can prevail on neither a deletion- nor an alteration-based trespass claim.

defendant actually has “induc[ed] or caus[ed]” a breach of contract, *Dunlap v. Cottman Transmission Sys., LLC*, 754 S.E.2d 313, 318 (Va. 2014) (quoting *Chaves v. Johnson*, 335 S.E.2d 97, 102 (Va. 1985)), taking affirmative action that is the proximate cause of the breach. See *Lockheed Info. Mgmt. Sys. Co. v. Maximus, Inc.*, 524 S.E.2d 420, 432–33 (Va. 2000).

OpenRisk does not dispute the district court’s evaluation of the record evidence so much as it advances a different legal ground for recovery: According to OpenRisk, it is enough that MicroStrategy’s actions “open[ed] up the door” to the former officers’ alleged breaches of contract, making it possible for them to use OpenRisk’s data. Br. of Appellant OpenRisk at 55. That but-for causation theory, however, is plainly inconsistent with Virginia law, which requires causation of the more direct and proximate variety. See *Lockheed*, 524 S.E.2d at 432–33. And this is not surprising. Under OpenRisk’s expansive alternative theory, liability could attach to any third-party vendor that does business with a company’s ex-employees and thus makes it possible for them to breach a post-employment contractual duty – by, for instance, providing them computer terminals or servicing a copier. OpenRisk can point to no Virginia case taking such a broad approach to tortious interference, and we have found none.<sup>5</sup>

---

<sup>5</sup> On appeal, OpenRisk argues that MicroStrategy committed tortious interference not only by making it possible for its former officers to breach post-employment contractual obligations, but also by inducing them to resign in the first instance. As OpenRisk concedes, it did not raise that argument before the district court until it filed a motion for reconsideration, which the district court denied without analysis. Accordingly, the argument has not been preserved for appellate review, and we do not address it. See *Holland v. Big River Minerals Corp.*, 181 F.3d 597, 605 (4th Cir. 1999).

Finally, OpenRisk argues that the district court erred in granting summary judgment to MicroStrategy on its claims for Virginia common law and statutory business conspiracy. The district court relied on two alternative and independent grounds for its decision: first, that OpenRisk had failed to proffer evidence from which a reasonable factfinder could conclude that MicroStrategy had engaged in an agreement to harm OpenRisk; and, second, that the conspiracy claims were based on underlying predicate acts preempted by federal law.

We begin – and may end – with the district court’s second rationale. Under Virginia law, OpenRisk can succeed on either of its conspiracy claims only if it has “sustained damages as a result of an act that is itself wrongful or tortious.” *Dunlap*, 754 S.E.2d at 317. “If the underlying tort is dismissed for any reason, so, too, must the corresponding conspiracy claim be dismissed.” *Tire Eng’g & Distrib., LLC*, 682 F.3d at 311 (Virginia civil conspiracy); *see also Shirvinski v. U.S. Coast Guard*, 673 F.3d 308, 321 (4th Cir. 2012) (Virginia business conspiracy). As the district court explained, that rule entitles MicroStrategy to judgment as a matter of law on OpenRisk’s conspiracy claims because – as the district court held and we now affirm – the state-law violations on which they are predicated are preempted by the Copyright Act.

On appeal, OpenRisk argues that the district court misunderstood its complaint, which in fact alleges as predicates not only the conversion, embezzlement, and larceny claims deemed preempted by the district court but also unlawful deletion under the VCCA and tortious interference. We need not decide whether OpenRisk’s reading of the complaint – which is not apparent on its face – could be sustained. As OpenRisk

recognizes, its argument could justify reinstatement of its conspiracy claims only if one or both of the potential additional predicates to which it points were improperly dismissed by the district court. But as set forth above, the district court properly awarded summary judgment on those claims, too. Because no possible predicate claim survives, the district court correctly held that OpenRisk cannot prevail on its conspiracy claims for that reason alone.

### **III.**

For the foregoing reasons, we affirm the judgment of the district court.

*AFFIRMED*