UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

─────────

No. 15-2301

─────────

FIRST DATA MERCHANT SERVICES CORPORATION, a Florida corporation; FIRST DATA CORPORATION,

Plaintiffs – Appellees,

v.

SECURITYMETRICS, INC., a Utah corporation,

Defendant – Appellant.

─────────

No. 15-2364

─────────

FIRST DATA MERCHANT SERVICES CORPORATION, a Florida corporation; FIRST DATA CORPORATION,

Plaintiffs – Appellants,

v.

SECURITYMETRICS, INC., a Utah corporation,

Defendant - Appellee.

─────────

Appeals from the United States District Court for the District of Maryland, at Baltimore. Richard D. Bennett, District Judge. (1:12-cv-02568-RDB)

─────────

Argued: October 25, 2016   Decided: December 1, 2016

─────────

Before SHEDD, DUNCAN, and FLOYD, Circuit Judges.

Affirmed by unpublished opinion. Judge Duncan wrote the opinion, in which Judge Shedd and Judge Floyd joined.

ARGUED: Lannie Rex Sears, MASCHOFF BRENNAN LAYCOCK GILMORE ISRAELSEN & WRIGHT PLLC, Salt Lake City, Utah, for Appellant/Cross-Appellee. Michael Lee Eidel, FOX ROTHSCHILD LLP, Philadelphia, Pennsylvania, for Appellees/Cross-Appellants.
ON BRIEF: Sterling A. Brennan, MASCHOFF BRENNAN LAYCOCK GILMORE ISRAELSEN & WRIGHT PLLC, Salt Lake City, Utah; J. Stephen Simms, SIMMS SHOWERS, LLP, Baltimore, Maryland, for Appellant/Cross-Appellee. Joshua Horn, Clair E. Wischusen, FOX ROTHSCHILD LLP, Philadelphia, Pennsylvania; Charles N. Curlett, Jr., LEVIN & CURLETT LLC, Baltimore, Maryland, for Appellees/Cross-Appellants.

Unpublished opinions are not binding precedent in this circuit.

DUNCAN, Circuit Judge:

First Data Merchant Services Corporation and First Data Corporation (collectively, "First Data") and SecurityMetrics, Inc. ("SecurityMetrics"), business partners turned adversaries, bring this appeal and cross-appeal challenging two orders of the district court. Throughout this protracted litigation, the parties have asserted numerous claims against each other, but only four are at issue here. SecurityMetrics appeals three counterclaims on which the district court granted First Data summary judgment on December 30, 2014 (the "December Order"). First Data cross-appeals the district court's denial of attorneys' fees in an order dated September 22, 2015 (the "September Order"). For the reasons discussed below, we affirm both orders.

I.

A.

First Data and SecurityMetrics are both companies in the Payment Card Industry ("PCI"). The PCI includes three types of primary service providers. Issuers supply payment cards to consumers and collect amounts due; acquirers clear and settle payment card transactions on behalf of merchants; and processors facilitate the communication and settlement of payment. Some PCI providers outsource certain functions to third-party

vendors.   First Data performs both acquirer and processor

functions.   SecurityMetrics is a third-party vendor.

The PCI Security Standards Council, an independent body

created by the five major payment card brands,[1] issues a set of

security standards, called the PCI Data Security Standard ("PCI

Standard" or "PCI DSS") to help protect against credit card

theft and fraud.   The PCI Standard is universal but the payment

card brands each have different requirements for demonstrating

or validating compliance with the standard.   Level 4 merchants--

the   category   at   issue   here--have   the   lowest   individual

transaction volume and are required to submit annual self-

assessment questionnaires to demonstrate compliance.

Any merchant that accepts credit payments must adhere to

the PCI Standard.   Acquirers, like First Data, must ensure that

their merchants comply with the PCI Standard and can impose

noncompliance penalties and fees on merchants.   Acquirers often

rely   on   third-party   vendors,   such   as   SecurityMetrics,   to

validate their merchants' compliance.

B.

From 2008 until 2012 the parties worked together pursuant

to a series of contracts.   Under the terms of the agreements,

First   Data   listed   SecurityMetrics   as   its   preferred   data

---

[1] American Express, Discover, JCB, MasterCard, and Visa.

compliance vendor in all communications with First Data's Level 4 merchants. First Data charged merchants a PCI compliance fee and then paid SecurityMetrics for its compliance services on behalf of the merchants. SecurityMetrics provided First Data with a weekly data feed and access to SecurityMetrics's system so that First Data could track the compliance status of its merchants.

This arrangement continued without issue until First Data decided to offer its own compliance service in 2012.[2] In preparation for the launch of its service, First Data ordered SecurityMetrics to cease communication with its Level 4 merchants effective June 1, 2012. In response, SecurityMetrics alleged First Data had breached their contract and stopped sending its weekly data feed.

C.

In May 2012, First Data filed suit against SecurityMetrics in the United States District Court for the District of Utah (the "Utah litigation") alleging breach of contract and other tortious conduct. The parties settled the Utah litigation pursuant to a document titled "Terms of Settlement." Under the

---

[2] During the course of this litigation, First Data wound down its proprietary compliance service and began to use a different third-party PCI compliance vendor, Trustwave. Trustwave became First Data's preferred PCI compliance vendor.

Terms of Settlement, the parties agreed to a few basic provisions that were to be memorialized in a confidential final settlement agreement that would include "mutual non-disparagement provisions." J.A. 217. First Data agreed to pay SecurityMetrics $5,000,000 and dismiss the Utah litigation with prejudice, and SecurityMetrics was granted the "use of Merchant Data for the purpose of selling its products and services." Id.

A final settlement agreement never materialized. Less than three months after signing the Terms of Settlement, First Data filed the underlying action against SecurityMetrics in the United States District Court for the District of Maryland. First Data alleged nine counts of post-settlement misconduct against SecurityMetrics.[3] SecurityMetrics answered and asserted fifteen counterclaims.[4] The parties filed cross-motions for

---

[3] First Data asserted the following counts: (1) Declaratory relief as to the definition of Merchant Data; (2) Breach of Contract of the Terms of Settlement; (3) Common Law Unfair Competition; (4) Tortious Interference with Existing and Prospective Contractual and Business Relationships; (5) Injurious Falsehoods; (6) False Endorsement/Association, Lanham Act, 15 U.S.C. § 1125(a)(1)(A); (7) Trademark/Service Mark/Trade Name Infringement, Lanham Act, 15 U.S.C. §§ 1114(1), 1125(a)(1)(A); (8) False Advertising, Lanham Act, 15 U.S.C. § 1125(a)(1)(B); and (9) Declaratory Relief as to PCI compliance reporting data.

[4] SecurityMetrics alleged First Data had, through its advertisements and communications with merchants, disparaged SecurityMetrics and brought the following counterclaims: (1) Specific Performance of the provision in the Terms of Settlement to execute a final settlement agreement; (Continued)

summary judgment, and the district court held a hearing on the motions and issued the December Order. In the December Order, the district court denied SecurityMetrics's motion for summary judgment but granted First Data's motion for summary judgment as to Counts 4 through 15 of SecurityMetrics's counterclaims.

The district court scheduled a trial as to the remaining claims. On the eve of trial, the parties narrowed the claims down to the sole issue of the meaning of the term "Merchant Data" in the Terms of Settlement. Following a two-day bench trial, the district court ruled in favor of SecurityMetrics.

After the trial, First Data filed a motion for attorneys' fees in relation to SecurityMetrics's Utah Truth in Advertising Act ("UTIAA") claim (Count 8) on which the district court had granted First Data summary judgment in the December Order. The UTIAA provides that "[t]he court shall award attorneys' fees to the prevailing party" in a UTIAA action. Utah Code § 13-11a-

_____

(2) Declaratory Judgment with respect to the Merchant Data provision of the Terms of Settlement; (3) Declaratory Judgment with respect to the confidentiality clause of the Terms of Settlement; (4) Injurious Falsehoods; (5) Federal False Advertising; (6) Federal False Endorsement; (7) Cancellation of Registration; (8) Utah Deceptive Trade Practices violations; (9) Tortious Interference with Business Relations; (10) Federal Restraint of Trade; (11) Federal Monopolization and Attempted Monopolization; (12) Maryland Restraint of Trade; (13) Maryland Monopolization and Attempted Monopolization; (14) Maryland Predatory Pricing; (15) Anticompetitive pricing arrangements in violation of Md. Code Com. Law § 11-204(a)(6).

4(2)(c). The district court denied this motion in the September Order finding that, although First Data did prevail as to the UTIAA claim itself, it was not a "prevailing party" at trial and with respect to the litigation as a whole.

<div align="center">D.</div>

On appeal, the parties do not contest the district court's ruling at trial as to the meaning of the term Merchant Data. Rather, the claims at issue before us originate from the pretrial December Order. SecurityMetrics appeals three of its counterclaims that the district court dismissed.

First, SecurityMetrics alleges First Data's advertisements violated the Lanham Act. Certain First Data promotional materials stated its merchants would have to pay First Data's compliance fee regardless of whether the merchant also used a third-party compliance vendor. SecurityMetrics claims this is a false statement because First Data actually provided refunds to merchants who used third-party compliance vendors. Finding the statements were literally true, the district court granted First Data summary judgment on this claim.

Second, SecurityMetrics contends First Data tortiously interfered with its business relations by making disparaging comments to merchants about SecurityMetrics. The district court also granted First Data summary judgment as to this claim

because it found that SecurityMetrics had not offered any admissible evidence to establish causation.

Third, SecurityMetrics challenges the district court's ruling as to its antitrust claims. SecurityMetrics alleged that First Data violated several antitrust laws when it launched its own competing PCI compliance service. The district court found that, because SecurityMetrics had not demonstrated injury to competition, rather than simply injury to itself, it lacked standing to pursue those claims. The court therefore granted First Data summary judgment as to these claims.

First Data cross-appeals the district court's denial of attorneys' fees as to SecurityMetrics's failed UTIAA claim. We first consider SecurityMetrics's claims in turn and then evaluate First Data's cross-appeal. For the reasons that follow, we affirm the district court's rulings on both parties' claims.

II.

Summary judgment is appropriate when "there is no genuine dispute as to any material fact." Fed. R. Civ. P. 56(a). We review the district court's grant of summary judgment de novo, viewing the facts and drawing all reasonable inferences in the light most favorable to the nonmovant. Askew v. HRFC, LLC, 810 F.3d 263, 266 (4th Cir. 2016). In doing so, "it is ultimately

the nonmovant's burden to persuade us that there is indeed a dispute of material fact. It 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." CorTel Va., LLC v. Verizon Va., LLC, 752 F.3d 364, 370 (4th Cir. 2014) (citation omitted). Regardless of the standard imposed by the burden of persuasion, the nonmovant may not defeat a motion for summary judgment "without offering any concrete evidence from which a reasonable juror could return a verdict in his favor [nor] by merely asserting the jury might, and legally could," disbelieve the movant. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 256 (1986).

III.

A.

We first consider whether the district court erred in granting summary judgment to First Data on its false advertising claim. We conclude it did not.

To bring a false advertising claim under the Lanham Act, a plaintiff must establish that (1) the defendant made a false or misleading description of fact or representation of fact in a commercial advertisement about his own or another's product that (2) is material and (3) actually deceives or has the tendency to deceive a substantial segment of its audience (4) after being

placed in interstate commerce, (5) causing the plaintiff injury. PBM Prods., LLC v. Mead Johnson & Co., 639 F.3d 111, 120 (4th Cir. 2011).

Only the first element--whether First Data's advertisements were false or misleading--is at issue here. A plaintiff can establish the first element by showing an advertisement is either (a) literally false or (b) literally true but likely to mislead or confuse consumers. C.B. Fleet Co. v. SmithKline Beecham Consumer Healthcare, L.P., 131 F.3d 430, 434 (4th Cir. 1997). SecurityMetrics proceeds on the first theory.

"In analyzing whether an advertisement . . . is literally false, a court must determine, first, the unambiguous claims made by the advertisement . . . and, second, whether those claims are false." PBM Prods., 639 F.3d at 120 (quoting Scotts Co. v. United Indus. Corp., 315 F.3d 264, 274 (4th Cir. 2002)). "A literally false message may be either explicit or conveyed by necessary implication when, considering the advertisement in its entirety, the audience would recognize the claim as readily as if it had been explicitly stated." Id. (quoting Scotts Co., 315 F.3d at 274). A false-by-necessary-implication claim must fail if the advertisement "can reasonably be understood as conveying different messages." Scotts Co., 315 F.3d at 275. "Only an unambiguous message can be literally false." Id. at 275-76 (quoting Novartis Consumer Health, Inc. v. Johnson & Johnson-

11

Merck Consumer Pharm. Co., 290 F.3d 578, 587 (3d Cir. 2002)

(emphasis in original)).

The challenged First Data advertisements state:

> If you choose to use a third-party vendor for PCI
> DSS compliance services, you will need to contract
> with and pay that vendor directly. <u>In addition</u> to
> your alternate vendor's charges for PCI DSS compliance
> services, you still will need to pay the Compliance
> Service Fee charged to you by your merchant services
> provider. <u>The Compliance Service Fee is not affected
> by your choice to use a third-party vendor</u>.

<div align="center">* * *</div>

> If First Data's PCI compliance services are
> contractually available to you, you will be charged an
> applicable annual compliance fee for those services,
> regardless of whether you use them or utilize the
> services of some other third-party PCI compliance
> services vendor. If you utilize the additional
> services of a third party vendor, you will pay that
> third party vendor's charges for those fees <u>in
> addition</u> to First Data's annual compliance fee.

J.A. 799–800 (emphasis added). According to SecurityMetrics,

these advertisements are literally false because First Data

refunded some merchants that paid both the First Data PCI

compliance fee and a third-party vendor. Because the

advertisements can, in context, be read more than one way,

however, we reject SecurityMetrics's argument.

It is undisputed that First Data has always charged its

merchants a PCI compliance fee. When the parties worked

together under their contract, First Data would pay

SecurityMetrics from the PCI compliance fee charged to the

<div align="center">12</div>

merchants.   Once SecurityMetrics was no longer a preferred

vendor, as the advertisements state, First Data still required

its merchants to pay its PCI Compliance fee.   If the merchant

used First Data's PCI compliance services, the merchant would

not pay anything additional.   If, however, a merchant wished to

use a third-party compliance vendor--such as SecurityMetrics--

the merchant would have to pay that fee directly to the third

party.   Hence, a merchant would pay for compliance services

twice.   SecurityMetrics contends that, though this was First

Data's official policy, in practice First Data would refund a

merchant that complained about being double charged in the

amount of the SecurityMetrics fee.   Therefore, SecurityMetrics

argues, the advertisement necessarily implies a literal

falsehood.   The district court disagreed and found these

statements were "only problematic due to what was left unsaid--

that a refund might be available."   J.A. 1369.   We agree.[5]

---

[5] SecurityMetrics also objects that, on the motion for
summary judgment, the district court "without warning or other
intervening change in circumstances" changed course from an
earlier position. Appellant's Br. at 15. When First Data moved
to dismiss the false advertising claim, the district court found
that the claim was "articulable as an affirmative misstatement--
i.e., that merchants will pay for the service but that some do
not because of the refund."   J.A. 229-30.   SecurityMetrics
alleges the district court erred in subsequently dismissing the
claim.   Of   course   this   argument   ignores   the   fundamental
difference between attacking a claim on a motion to dismiss and
at the summary judgment stage.   In a motion to dismiss, the
court must accept the factual allegations in the plaintiff's
(Continued)

First Data's advertisements are not unambiguous and therefore cannot be literally false. On one reading of the advertisement, the service fee <u>is</u> affected because First Data would, if asked, refund customers an amount equal to the third-party vendor charge. Merchants who asked for and received a refund did not pay the third-party fee in addition to the PCI compliance fee. However, by another reading, because First Data's refund policy was discretionary and not automatic, the advertisement is true on its face. Put another way, if a SecurityMetrics customer never asked First Data for a refund, it would, as the advertisement states, pay a third-party vendor fee "in addition to" First Data's PCI Compliance fee. J.A. 799. A claim that is "implicit, attenuated, or merely suggestive usually cannot fairly be characterized as literally false." <u>Design Res., Inc. v. Leather Indus. of Am.</u>, 789 F.3d 495, 502 (4th Cir. 2015) (quoting <u>Clorox Co. P.R. v. Proctor & Gamble Commercial Co.</u>, 228 F.3d 24, 35 (1st Cir. 2000)). SecurityMetrics "asks us to reach entirely outside the face of

---

complaint as true. <u>Bell Atlantic Corp. v. Twombly</u>, 550 U.S. 544, 555 (2007). However, a plaintiff has a higher burden when faced with a motion for summary judgment. At that stage of litigation, the party opposing summary judgment "must set forth specific facts showing that there is a genuine issue for trial." <u>Liberty Lobby</u>, 477 U.S. at 256 (internal citation omitted). SecurityMetrics failed to carry its burden.

14

the ad and into the context surrounding the ad's publication to uncover a false message it argues is necessarily implied," Id. at 503, but the false-by-necessary-implication doctrine does not stretch that far. Therefore, the district court properly granted First Data summary judgment on that issue.[6]

B.

SecurityMetrics next argues that the district court erred in granting First Data summary judgment as to the tortious interference claim. Under Maryland law, tortious interference with economic relations requires a claimant to show "(1) intentional and willful acts; (2) calculated to cause damage to the plaintiffs in their lawful business; (3) done with the unlawful purpose to cause such damage and loss, without right or justifiable cause on the part of the defendants (which constitutes malice); and (4) actual damage and loss resulting." Alexander & Alexander Inc. v. B. Dixon Evander & Assocs., Inc., 650 A.2d 260, 269 (Md. 1994) (quoting Willner v. Silverman, 71 A. 962, 964 (Md. 1909)). Because SecurityMetrics failed to establish causation, the district court granted First Data

---

[6] SecurityMetrics also argues that a jury must decide whether the statements were literally false. That is incorrect. Although literal falsity is a question of fact, C.B. Fleet Co., 131 F.3d at 436, whether a nonmovant has put forth sufficient evidence to establish a genuine dispute as to that fact is a legal question for the district court's determination. See Design Res., 789 F.3d at 502.

summary judgment on the tortious interference claim. We affirm for the same reason.

SecurityMetrics alleged First Data used the Utah litigation as "a weapon . . . for the . . . purpose of interfering with SecurityMetrics's actual and prospective economic relations." J.A. 194. According to SecurityMetrics, it lost 280,000 existing customers as well as potential new customers because of this alleged misconduct. SecurityMetrics sought to introduce two forms of evidence to show causation: (1) transcripts of phone calls and emails from customers stating why they were canceling or not renewing their contracts with SecurityMetrics and (2) an expert report prepared by Clarke Nelson (the "Nelson report"). The district court excluded both pieces of evidence.

The viability of SecurityMetrics's argument depends on whether the district court properly refused to admit the customer calls and emails and the Nelson report. We review the district court's rulings on the admissibility of evidence for abuse of discretion and will only reverse if the ruling was arbitrary and irrational. Minter v. Wells Fargo Bank, N.A., 762 F.3d 339, 349 (4th Cir. 2014). We find no abuse of discretion here.

1.

First, the district court did not err in excluding the customer communications as inadmissible hearsay. SecurityMetrics asserts the calls and emails should have been admitted either because they are verbal acts, and therefore not hearsay, or under the state of mind exception to the hearsay rule.

Under the Federal Rules of Evidence, verbal acts--those declarations where "the statement itself affects the legal rights of the parties or is a circumstance bearing on conduct affecting their rights"--are not hearsay. Fed. R. Evid. 801 advisory committee's note to subdivision (c). "[P]roof of oral utterances by the parties in a contract suit constituting <u>the offer and acceptance which brought the contract into being</u> are not evidence of assertions offered testimonially but rather verbal conduct to which the law attaches duties and liabilities." 2 McCormick on Evidence § 249 (7th ed.) (2016) (emphasis added).

Although portions of the calls and emails--references to contract terminations and account closure instructions--might constitute verbal acts, these admissible sections are not evidence of the causation element necessary to support SecurityMetrics's tortious interference claim. What SecurityMetrics wants to use from the calls--comments made by

customers regarding First Data's conduct--are not verbal acts. In other words, the existence of the contract is a verbal act but irrelevant to causation; the portions that would go to causation--why the merchants decided not to renew or sign a contract--are relevant but inadmissible.

Nor can the calls and recordings be admitted under the state of mind exception to hearsay. That exception excludes from hearsay "[a] statement of the declarant's then-existing state of mind . . . but not including a statement of memory or belief to prove the fact remembered or believed unless it relates to the validity or terms of the declarant's will." Fed. R. Evid. 803(3). SecurityMetrics attempts to avail itself of this exception by stating that the calls and emails are offered only to prove "what customers believed and why they did what they did." Appellant's Br. at 52. However, unless the statements are also offered for the truth of the matter asserted--that the merchants canceled their contracts with SecurityMetrics because of First Data's misconduct--these customer statements do not show causation.

Put simply, to escape a hearsay exclusion, SecurityMetrics could only offer the evidence for purposes irrelevant to demonstrating causation. The relevant evidence is inadmissible hearsay. Therefore, the district court did not abuse its

discretion in determining that no admissible portion of the calls and emails satisfied the element of causation.

2.

SecurityMetrics's argument as to the Nelson report is also unavailing. On appeal, SecurityMetrics faults the district court for not considering its expert's report as evidence of causation. However, SecurityMetrics retained Mr. Nelson as an expert to opine on the amount of damages, not causation. In Mr. Nelson's deposition in connection with First Data's motion in limine to exclude the report, he stated he did not "intend to give an opinion on causation . . . from a legal standpoint," but he did "intend to express opinions that" a "correlation" existed between First Data's "alleged bad acts and harm that was suffered." J.A. 1027–28. Upon further questioning, Mr. Nelson reiterated that he was not going to offer an opinion at trial as to whether "the alleged bad acts by First Data caused any damage." J.A. 1903. Therefore, the district court did not abuse its discretion by disregarding the Nelson report since it was not offered to prove any opinion on causation.

C.

Next, we turn to SecurityMetrics's antitrust counts. SecurityMetrics asserted six antitrust counterclaims against

19

First Data under federal and Maryland law.[7] To proceed on any of its claims, SecurityMetrics must first establish antitrust standing, which requires some cognizable antitrust injury. Brunswick Corp. v. Pueblo Bowl-O-Mat, Inc., 429 U.S. 477, 489 (1977). "Because the antitrust laws are intended to protect competition, and not simply competitors, only injury caused by damage to the competitive process may form the basis of an antitrust claim." Thompson Everett, Inc. v. Nat'l Cable Adv., L.P., 57 F.3d 1317, 1325 (4th Cir. 1995). SecurityMetrics alleged antitrust injury in the form of reduced output and frustrated price competition. The district court correctly rejected those claims because SecurityMetrics failed to support either theory with sufficient evidence to survive a motion for summary judgment.

As an initial matter, we note SecurityMetrics did not properly plead its antitrust claims because it did not allege any antitrust injury before the summary judgment stage. Generally, a party may not raise new arguments after discovery without amending its complaint. U.S. ex rel. Owens v. First Kuwaiti Gen. Trading & Contracting Co., 612 F.3d 724, 731 (4th Cir. 2010). SecurityMetrics argues that it did not need to

---

[7] Federal antitrust analysis also applies to SecurityMetrics's state law claims. See Md. Code § 11-202(a)(2).

20

plead which theory it would rely upon. Even assuming that is correct, SecurityMetrics was required to allege some antitrust injury, which its complaint did not.

Even if SecurityMetrics did properly plead its antitrust claims, they nonetheless fail. SecurityMetrics's evidence for its antitrust claims consisted of a wholly undeveloped claim that it lost 280,000 customers in two years, 70,000 of which went to First Data. SecurityMetrics points to the remaining unaccounted for 210,000 merchants as evidence of reduced output. SecurityMetrics provides no evidence to support its speculation that these "lost merchants" resulted from misconduct on the part of First Data. Any number of reasons might similarly explain the merchants' departure, all of which are conjecture.[8] The merchants could have migrated to a company other than First Data or SecurityMetrics, gone out of business altogether, changed their business mode, or no longer been in the market for a number of other reasons unrelated to First Data's alleged conduct. SecurityMetrics's "tenuous" inferences are simply not enough to "fall within the range of reasonable probability" and

---

[8] SecurityMetrics claims only First Data had access to the evidence related to the "lost merchants," leaving SecurityMetrics with the sole option of deposing 210,000 third parties to show reduced output. This argument, of course, overlooks the possibility that SecurityMetrics could have retained an expert to opine on the issue of reduced output.

overcome a summary judgment challenge. Thompson Everett, 57
F.3d at 1323. The district court therefore properly rejected
reduced output as a plausible antitrust injury.

SecurityMetrics's attempt to establish antitrust standing
based on harm to price competition fails for the same reason.
SecurityMetrics claims that although First Data's prices are
higher than SecurityMetrics, First Data has gained customers
while SecurityMetrics has lost them. It is unclear what harm to
price competition this fact reflects. SecurityMetrics does not
allege predatory pricing, which is the only pricing practice
that "has the requisite anticompetitive effect." Atlantic
Richfield Co. v. USA Petroleum Co., 495 U.S. 328, 340 (1990).
SecurityMetrics may have shown injury to its business but the
record lacks any evidence that First Data's practices harmed the
"competitive process." Thompson Everett, 57 F.3d at 1325. We
must therefore conclude that its antitrust claims fail.

IV.

Finally, we consider First Data's sole issue on cross-
appeal: the district court's denial of its attorneys' fees as it
relates to SecurityMetrics's UTIAA counterclaim. We review the
denial of attorneys' fees for abuse of discretion. Reinbol v.
Evers, 187 F.3d 348, 362 (4th Cir. 1999). We apply Utah law to
determine whether an award of attorneys' fees to First Data is

22

warranted. See Hitachi Credit Am. Corp. v. Signet Bank, 166 F.3d 614, 631 (4th Cir. 1999). "[W]e defer to the trial court's judgment, and reverse a trial court's attorney fees determination only if the trial court exceeds the bounds of its discretion." Neff v. Neff, 247 P.3d 380, 399 (Utah 2011).

SecurityMetrics brought a counterclaim under the UTIAA, which was enacted "to prevent deceptive, misleading, and false advertising practices and forms in Utah." Utah Code § 13-11a-1. The district court granted First Data summary judgment as to this claim because "the relevant provisions of the [UTIAA] track the Lanham Act [so] SecurityMetrics' claims under the state statute fail as well." J.A. 1372.[9] Under the UTIAA, "[t]he court shall award attorneys' fees to the prevailing party." Utah Code § 13-11a-4(2)(c). Notwithstanding the statutory language, the district court did not award First Data attorneys' fees because it was not the prevailing party "within the context of the case as a whole." J.A. 1939. First Data argues the district court's decision was an error of law. We disagree.

The Supreme Court of Utah has not defined "prevailing party" specifically as to the UTIAA, but it has provided a general framework to ascertain the prevailing party in an action.

---

[9] SecurityMetrics did not appeal its UTIAA claim.

In Neff v. Neff, 247 P.3d 380 (Utah 2011), two brothers and one-time business partners became embroiled in litigation spanning more than six years. After trial, both parties sought attorneys' fees, which the trial court denied. Only one brother appealed. The Supreme Court of Utah affirmed the denial and held that a trial court "must base its decision [whether to award attorney fees] on a number of factors." Id. at 398.

> These factors include the language of the contract or statute that forms the basis of the attorney fees award, the number of claims brought by the parties, the importance of each of the claims relative to the entire litigation, and the amounts awarded on each claim. . . . Accordingly, it is possible that, in litigation where both parties obtain mixed results, neither party should be deemed to have prevailed for purposes of awarding attorney fees. This is true <u>even where the statutory language states that a prevailing party 'shall be entitled to' fees</u>.

Id. at 398–99 (emphasis added) (footnotes omitted).

Here, the district court properly applied the rationale and standard announced in Neff. Between the two parties, there were twenty-four claims before the district court. The district court granted First Data summary judgment as to eleven of the claims. The parties voluntarily dismissed or withdrew eleven other claims.[10] Though the district court granted First Data

---

[10] After various pre-trial motions, First Data had four remaining claims (Counts 1, 2, 4, and 9) and SecurityMetrics had two remaining claims (Counts 2 and 3). The Friday before trial, the parties reached a partial resolution to winnow the remaining claims down to the meaning of Merchant Data under the Terms of (Continued)

summary judgment on several claims, it "never ruled that the conduct of which SecurityMetrics complained was not actionable," but rather that SecurityMetrics had not met its evidentiary burdens. J.A. 1940. Out of the twenty-four counts, the sole issue at trial was the parties' competing claims as to the meaning of Merchant Data.

Under Neff, the "prevailing party" does not refer to a single count nor is it simply a matter of adding up which party won the most claims. The district court here determined that, while First Data did prevail as to the UTIAA claim, it "had only limited success when the case is considered as a whole." J.A. 1938. The interpretation of Merchant Data was the only issue at trial, an issue on which First Data suffered a "resounding loss." J.A. 1940. Considering the Neff factors, the district court determined First Data's UTIAA claim "occupied a peripheral position in the litigation as a whole." J.A. 1939. The district court did not abuse its discretion in so finding. First Data's argument that the plain language of the UTIAA "does not state prevailing party in the entire action" is plainly

---

Settlement (First Data Count 1 and SecurityMetrics Count 2). The parties filed a consent order to dismiss with prejudice the remaining claims (First Data Counts 2, 4, and 9 and SecurityMetrics Count 3), each side bearing their own costs and fees. The parties also withdrew their request for a jury trial.

foreclosed by <u>Neff</u>'s holding that a district court must consider "each of the claims relative to the entire litigation . . . even where the statutory language states that a prevailing party shall be entitled to fees." <u>Neff</u> 247 P.3d at 398–99 (internal citation omitted). Therefore, we affirm the district court's denial of attorneys' fees.

V.

On the record before us, SecurityMetrics did not present evidence of a genuine issue of material fact sufficient to survive a motion for summary judgment on its Lanham Act claim, tortious interference claim, or antitrust claims. The district court did not abuse its discretion in finding that First Data was not a prevailing party in the overall action and, therefore, not entitled to attorneys' fees under the UTIAA. For these reasons, the judgment of the district court is

<u>AFFIRMED</u>.