

LVRC HOLDINGS LLC, Plaintiff-Appellant, v. CHRISTOPHER BREKKA; EMPLOYEE BUSINESS SOLUTIONS INC.; CAROLYN QUAIN; STUART SMITH; BRAD GREENSTEIN; FRANK SZABO, Defendants-Appellees.

No. 07-17116

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

581 F.3d 1127; 2009 U.S. App. LEXIS 20439; 159 Lab. Cas. (CCH) P10,165; 29 I.E.R. Cas. (BNA) 1153

**March 13, 2009, Argued and Submitted, San Francisco, California
September 15, 2009, Filed**

PRIOR HISTORY: [1]**

Appeal from the United States District Court for the District of Nevada. D.C. No. CV-05-01026-KJD. Kent J. Dawson, District Judge, Presiding.

LVRC Holdings, LLC v. Brekka, 2007 U.S. Dist. LEXIS 73662 (D. Nev., Sept. 28, 2007)

DISPOSITION: AFFIRMED.

COUNSEL: Thomas G. Grace, Las Vegas, Nevada, for the plaintiff-appellant.

Norman H. Kirshman, Las Vegas, Nevada, for the defendant-appellees.

JUDGES: Before: M. Margaret McKeown and Sandra S. Ikuta, Circuit Judges, and James V. Selna, * District Judge. Opinion by Judge Ikuta.

* The Honorable James V. Selna, United States District Judge for the Central District of California, sitting by designation.

OPINION BY: Sandra S. Ikuta

OPINION

[*1128] IKUTA, Circuit Judge:

LVRC Holdings, LLC (LVRC) filed this lawsuit in federal district court against its former employee, Christopher Brekka, his wife, Carolyn Quain, and the couple's two consulting businesses, Employee Business Solutions, Inc., a Nevada corporation [*1129] (EBSN), and Employee Business Solutions, Inc., a Florida corporation (EBSF). LVRC alleged that Brekka violated the Computer Fraud and Abuse Act (CFAA), *18 U.S.C. § 1030*, by accessing LVRC's computer "without authorization," both while Brekka was employed at LVRC and after he left the company. *See 18 U.S.C. § 1030(a)(2), (4)*. The district court granted summary judgment in favor of the defendants. [**2] We affirm. Because Brekka was authorized to use LVRC's computers while he was employed at LVRC, he did not access a computer "without authorization" in violation of *§ 1030(a)(2)* or *§ 1030(a)(4)* when he emailed documents to himself and to his wife prior to leaving LVRC. Nor did emailing the documents "exceed authorized access," because Brekka was entitled to obtain the documents. Further, LVRC failed to establish the existence of a genuine issue of material fact as to whether

Brekka accessed the LVRC website without authorization after he left the company.

I

LVRC operates Fountain Ridge, a residential treatment center for addicted persons, in Nevada. ¹ As part of its marketing efforts, LVRC retained LOAD, Inc. to provide email, website, and related services for the facility. Among other duties, LOAD monitored internet traffic to LVRC's website and compiled statistics about that traffic.

1 Because this appeal comes to us from the grant of a motion for summary judgment, we relate the facts in the light most favorable to LVRC. *See Nolan v. Heald College*, 551 F.3d 1148, 1150 (9th Cir. 2009).

In April 2003, LVRC hired Brekka to oversee a number of aspects of the facility. Part of his duties included **[**3]** conducting internet marketing programs and interacting with LOAD. At the time Brekka was hired, Brekka owned and operated EBSN and EBSF, two consulting businesses that obtained referrals for addiction rehabilitation services and provided referrals of potential patients to rehabilitation facilities through the use of internet sites and advertisements. Stuart Smith, the owner and operator of LVRC, was aware of Brekka's businesses, although he states he was not aware of the full nature of their operations.

While Brekka worked for LVRC, he commuted between Florida, where his home and one of his businesses were located, and Nevada, where Fountain Ridge and his second business were located. Brekka was assigned a computer at LVRC, but while commuting back and forth between Florida and Nevada, he emailed documents he obtained or created in connection with his work for LVRC to his personal computer. LVRC and Brekka did not have a written employment agreement, nor did LVRC promulgate employee guidelines that

would prohibit employees from emailing LVRC documents to personal computers.

In June 2003, Brekka sent an email to LOAD's administrator, Nick Jones, requesting an administrative log-in for **[**4]** LVRC's website. Jones sent an email with the administrative user name, "cbrekka@fountainridge.com," and password, "cbrekka," to Brekka's work email, which Brekka downloaded onto his LVRC computer. By using the administrative log-in, Brekka gained access to information about LVRC's website, including the usage statistics gathered by LOAD. Brekka used those statistics in managing LVRC's internet marketing.

In August 2003, Brekka and LVRC entered into discussions regarding the possibility of Brekka purchasing an ownership interest in LVRC. At the end of August 2003, Brekka emailed a number of LVRC documents to his personal **[*1130]** email account and his wife's personal email account. These documents included a financial statement for the company, LVRC's marketing budget, admissions reports for patients at Fountain Ridge, and notes Brekka took from a meeting with another Nevada mental health provider. On September 4, 2003, Brekka emailed a master admissions report, which included the names of past and current patients at Fountain Ridge, to his personal email account.

In mid-September 2003, negotiations regarding Brekka's purchase of an ownership interest in LVRC broke down, and Brekka ceased working **[**5]** for LVRC. Brekka left his LVRC computer at the company and did not delete any emails from the computer, so the June 2003 email from Nick Jones, which included the administrative user name and password, remained on his computer.

After Brekka left the company, other LVRC employees had access to Brekka's former computer, including Brad Greenstein, a consultant who was hired shortly before Brekka left and

who assumed many of Brekka's responsibilities. At some point after Brekka left, the email with the administrative log-in information was deleted from his LVRC computer.

On November 19, 2004, while performing routine monitoring of the LOAD website, Jones noticed that someone was logged into the LVRC website using the user name "cbrekka@fountainridge.com" and was accessing LVRC's LOAD statistics. Jones contacted Greenstein about the use of the "cbrekka" log-in. Jones also provided the IP address of the log-in and the location of the Internet Service Provider (ISP) associated with that IP address, namely, Redwood City, California. Greenstein instructed Jones to deactivate the "cbrekka" log-in, and Jones did so the same day. Shorting thereafter, LVRC filed a report with the FBI, alleging that [**6] Brekka had unlawfully logged into LVRC's website.

LVRC then brought an action in federal court, alleging that Brekka violated the CFAA when he emailed LVRC documents to himself in September 2003 and when he continued to access the LOAD website after he left LVRC. In addition, LVRC brought a number of state tort actions. In response, Brekka filed a third-party complaint against Smith, Greenstein, and Frank Szabo, alleging that they defamed him by making statements that Brekka had stolen information from LVRC.²

2 Brekka's third-party complaint against Smith, Greenstein, and Frank Szabo is not on appeal before us.

The district court granted summary judgment in favor of Brekka. After dismissing the federal law claims, the district court declined to exercise supplemental jurisdiction over the remaining state law claims and dismissed the case. LVRC filed a motion to reconsider. Before the district court ruled on the motion, LVRC filed this appeal. We review the district court's grant of a motion for summary judgment

de novo. *SDV/ACCI, Inc. v. AT&T Corp.*, 522 F.3d 955, 958 (9th Cir. 2008).

II

The CFAA was enacted in 1984 to enhance the government's ability to prosecute computer crimes. The act [**7] was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to "access and control high technology processes vital to our everyday lives" H.R. Rep. 98-894, [**1131] 1984 U.S.C.C.A.N. 3689, 3694 (July 24, 1984). The CFAA prohibits a number of different computer crimes, the majority of which involve accessing computers without authorization or in excess of authorization, and then taking specified forbidden actions, ranging from obtaining information to damaging a computer or computer data. *See* 18 U.S.C. β 1030(a)(1)-(7) (2004).³

3 The CFAA has been amended multiple times since 1984; for purposes of this case, the 1986 amendments are applicable. The act was amended again in 2008. *See* Pub. L. 110-326, $\beta\beta$ 203-08. Unless otherwise indicated, all citations in this opinion are to the 2004 U.S. Code, which contains the version of the CFAA in force during the relevant time period in this case.

LVRC's complaint alleged that Brekka committed two of the crimes established by the CFAA, 18 U.S.C. $\beta\beta$ 1030(a)(2) and (a)(4). Section β 1030(a)(2) provides for criminal penalties to [**8] be imposed on a person who:

intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains-- . . .

(C) information from any protected computer if the conduct in-

involved an interstate or foreign communication

18 U.S.C. § 1030(a)(2). Section 1030(a)(4) provides for criminal penalties to be imposed on a person who:

knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value

*18 U.S.C. § 1030(a)(4).*⁴

4 For purposes of these sections, a "protected computer" is defined as including any computer "used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." *18 U.S.C. § 1030(e)(2).*

LVRC brought suit under the provision of the statute that creates a right of action for private persons injured by such crimes. *Section 1030(g)* provides in pertinent part:

Any person who suffers damage or loss by reason of a violation of this section may maintain **[**9]** a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (I), (ii), (iii), (iv), or (v) of subsection (a)(5)(B).

18 U.S.C. § 1030(g). Thus, a private plaintiff must prove that the defendant violated one of the provisions of *§ 1030(a)(1)-(7)*, and that the violation involved one of the factors listed in *§ 1030(a)(5)(B)*.⁵ LVRC claims that Brekka's conduct involved the factor described in *subsection (a)(5)(B)(i)*, which proscribes conduct that causes "loss to 1 or more persons during any 1-year period . . . aggregating **[*1132]** at least \$ 5,000 in value." *18 U.S.C. § 1030(a)(5)(B)(i).*

5 The factors set forth in *§ 1030(a)(5)(B)(i)-(v)* are:

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$ 5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical **[**10]** examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security

. . . .

18 U.S.C. § 1030(a)(5)(B).

Therefore, to bring an action successfully under *18 U.S.C. § 1030(g)* based on a violation of *18 U.S.C. § 1030(a)(2)*, LVRC must show that Brekka: (1) intentionally accessed a computer, (2) without authorization or exceeding authorized access, and that he (3) thereby obtained information (4) from any protected computer (if the conduct involved an interstate or foreign communication), and that (5) there was loss to one or more persons during any one-year period aggregating at least \$ 5,000 in value. To bring an action successfully under *§ 1030(g)* based on a violation of *§ 1030(a)(4)*, LVRC must show that Brekka: (1) accessed a "protected computer," (2) without authorization or exceeding such authorization that was granted, (3) "knowingly" and with "intent to defraud," and thereby (4) "further[ed] the intended fraud and obtain[ed] anything of value," [**11] causing (5) a loss to one or more persons during any one-year period aggregating at least \$ 5,000 in value. *See 18 U.S.C. § 1030(a)*; *see also P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504, 508 (3d Cir. 2005); *Theofel v. Farey-Jones*, 359 F.3d 1066, 1078 (9th Cir. 2004).

In granting Brekka's summary judgment motion, the district court held that LVRC had failed to establish a violation of either *§ 1030(a)(2)* or (4). First, the district court stated that "[i]t is undisputed that when Brekka was employed by Plaintiff that he had authority and authorization to access the documents and emails that were found on his home computer and laptop." According to the district court, LVRC adduced no evidence demonstrating that Brekka accessed an LVRC computer or any of the documents on the computer "without authorization" (an element of both *§§ 1030(a)(2)* and (4)) when he emailed documents to himself and to his wife before he left the company. The district court based this rul-

ing on its conclusion that Brekka had "authorization" to access the LVRC computers for purposes of *§§ 1030(a)(2)* and (4) because he was employed by LVRC at the time he emailed documents [**12] to himself and his wife, and there was no evidence that Brekka had agreed to keep the emailed documents confidential or to return or destroy those documents upon the conclusion of his employment. Second, the district court held that LVRC had not put forth evidence from which a reasonable jury could find that Brekka logged into the LVRC website after leaving LVRC's employ. Because of the lack of evidence that Brekka violated *§ 1030(a)(2)* or (4), the district court dismissed LVRC's claim under *§ 1030(g)*.

LVRC disputes both of these determinations, and we address each in turn.

III

We first consider LVRC's argument that the district court erred in assuming that if Brekka's access occurred during the term of his employment, it must have been authorized for purposes of the CFAA. LVRC argues that because Brekka accessed the company computer and obtained LVRC's confidential information to further his own personal interests, rather than the interests of LVRC, such access was "without authorization" for purposes of *§§ 1030(a)(2)* and (4).

In interpreting the phrase "without authorization," we start with the plain language of the statute. *See United States v. Blixt*, 548 F.3d 882, 887 (9th Cir. 2008). [**13] The CFAA does not define "authorization," and it is a "fundamental canon of statutory construction . . . that, unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning." *Perrin v. United States*, 444 U.S. 37, 42, 100 S. Ct. 311, 62 L. Ed. 2d 199 [*1133] (1979); *see also United States v. Morris*, 928 F.2d 504, 511 (2d Cir. 1991) (holding that the word "authorization" for purposes of the CFAA is "of common us-

age, without any technical or ambiguous meaning," and therefore the district court "was not obliged to instruct the jury on its meaning"). Authorization is defined in the dictionary as "permission or power granted by an authority." RANDOM HOUSE UNABRIDGED DICTIONARY, 139 (2001); *see also* WEBSTER'S THIRD INTERNATIONAL DICTIONARY, 146 (2002) (defining authorization as "the state of being authorized" and "authorize" as "to endorse, empower, justify, permit by or as if by some recognized or proper authority"). Based on this definition, an employer gives an employee "authorization" to access a company computer when the employer gives the employee permission to use it. Because LVRC permitted Brekka to use the company computer, the "ordinary, contemporary, common meaning," *Perrin*, 444 U.S. at 42, [**14] of the statute suggests that Brekka did not act "without authorization."

No language in the CFAA supports LVRC's argument that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's interest. Rather, the definition of "exceeds authorized access" in β 1030(e)(6) indicates that Congress did not intend to include such an implicit limitation in the word "authorization." Section 1030(e)(6) provides: "the term 'exceeds authorized access' means to access 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." 18 U.S.C. β 1030(e)(6). As this definition makes clear, an individual who is authorized to use a computer for certain purposes but goes beyond those limitations is considered by the CFAA as someone who has "exceed[ed] authorized access." On the other hand, a person who uses a computer "without authorization" has no rights, limited or otherwise, to access the computer in question. In other words, for purposes of the CFAA, when an employer authorizes an employee to use a company computer subject to certain limitations, the employee [**15] re-

mains authorized to use the computer even if the employee violates those limitations. It is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or "without authorization."

This leads to a sensible interpretation of $\beta\beta$ 1030(a)(2) and (4), which gives effect to both the phrase "without authorization" and the phrase "exceeds authorized access": a person who "intentionally accesses a computer without authorization," $\beta\beta$ 1030(a)(2) and (4), accesses a computer without any permission at all, while a person who "exceeds authorized access," *id.*, has permission to access the computer, but accesses information on the computer that the person is not entitled to access.

In this case, there is no dispute that Brekka had permission to access the computer; indeed, his job required him to use the computer. *Cf. Theofel*, 359 F.3d at 1072-73 (holding that defendants had accessed a computer "without authorization" for purposes of the Stored Communications Act, 18 U.S.C. β 2701 *et seq.*, when they procured the access by fraud). Moreover, there is no dispute that Brekka was still employed by LVRC when he emailed the [**16] documents to himself and to his wife. The most straightforward interpretation of $\beta\beta$ 1030(a)(2) and (4) is that Brekka had authorization to use the computer.

LVRC attempts to counter this conclusion by pointing to a Seventh Circuit decision, *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006). According to LVRC, *Citrin* supports its argument that the CFAA incorporates an additional limitation in the word "authorization," [**1134] such that an employee can lose authorization to use a company computer when the employee resolves to act contrary to the employer's interest. In *Citrin*, the court held that an employee's authorization to access a computer ended for purposes of β 1030(a)(5) ⁶ when the employee violated his duty of loyalty to his employer. The employee

had decided to start a competing business in violation of his employment contract and erased all data from his work laptop computer before quitting his job. *Id.* at 419. The erased data included both valuable information belonging to his employer and evidence that the employee had engaged in misconduct. *Id.* The Seventh Circuit held that, under common law agency principles, the employee breached his duty of loyalty to **[**17]** his employer "when, having already engaged in misconduct and decided to quit [the company] in violation of his employment contract, he resolved to destroy files that incriminated himself and other files that were also the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee." *Id.* at 420. The court held that this breach of the duty of loyalty to his employer terminated the employee's agency relationship "and with it his authority to access the laptop, because the only basis of his authority had been that relationship." *Id.* at 420-21. Accordingly, the Seventh Circuit held that the employee's actions were "without authorization" for purposes of β 1030(a)(5). *Id.* at 421.

6 18 U.S.C. β 1030(a)(5) provides for criminal penalties to be imposed on a person who, among other things, "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage" or "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage."

If we applied the reasoning in *Citrin* to this case, Brekka would have breached his duty of loyalty to LVRC when he allegedly **[**18]** resolved to transfer key LVRC documents and information to his personal computer to further his own competing business, and at that point his authorization to access the computer would have ended. Applying this reasoning, Brekka would have acted "without authorization" for purposes of $\beta\beta$ 1030(a)(2) and (4) once his

mental state changed from loyal employee to disloyal competitor.

We are unpersuaded by this interpretation. First, and most important, β 1030 is primarily a criminal statute, and $\beta\beta$ 1030(a)(2) and (4) create criminal liability for violators of the statute. Although this case arises in a civil context, our interpretation of $\beta\beta$ 1030(a)(2) and (4) is equally applicable in the criminal context. See *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8, 125 S. Ct. 377, 160 L. Ed. 2d 271 (2004) (holding that where a statute "has both criminal and non-criminal applications," courts should interpret the statute consistently in both criminal and noncriminal contexts). It is well established that "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity." *United States v. Carr*, 513 F.3d 1164, 1168 (9th Cir. 2008) (quoting *Rewis v. United States*, 401 U.S. 808, 812, 91 S. Ct. 1056, 28 L. Ed. 2d 493 (1971)). The Supreme Court has long **[**19]** warned against interpreting criminal statutes in surprising and novel ways that impose unexpected burdens on defendants. See *United States v. Santos*, 128 S. Ct. 2020, 2025, 170 L. Ed. 2d 912 (2008) (J. Scalia) (plurality opinion) (citing *United States v. Bass*, 404 U.S. 336, 347-49, 92 S. Ct. 515, 30 L. Ed. 2d 488 (1971); *McBoyle v. United States*, 283 U.S. 25, 27, 51 S. Ct. 340, 75 L. Ed. 816 (1931); *United States v. Gradwell*, 243 U.S. 476, 485, 37 S. Ct. 407, 61 L. Ed. 857 (1917)). "This venerable rule . . . vindicates **[*1135]** the fundamental principle that no citizen should be held accountable for a violation of a statute whose commands are uncertain, or subjected to punishment that is not clearly prescribed." *Id.* Therefore, "[t]he rule of lenity, which is rooted in considerations of notice, requires courts to limit the reach of criminal statutes to the clear import of their text and construe any ambiguity against the government." *United States v. Romm*, 455 F.3d 990, 1001 (9th Cir. 2006).

In this case, as noted above, "authorization" means "permission or power granted by an

authority." RANDOM HOUSE UN-ABRIDGED DICTIONARY, 139. The definition of the term "exceeds authorized access" from β 1030(e)(6) implies that an employee can violate employer-placed limits on accessing information stored on the computer [**20] and still have authorization to access that computer. The plain language of the statute therefore indicates that "authorization" depends on actions taken by the employer. Nothing in the CFAA suggests that a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer. If the employer has not rescinded the defendant's right to use the computer, the defendant would have no reason to know that making personal use of the company computer in breach of a state law fiduciary duty to an employer would constitute a criminal violation of the CFAA. It would be improper to interpret a criminal statute in such an unexpected manner. *See Carr*, 513 F.3d at 1168.

Because LVRC's proposed interpretation based on *Citrin* does not comport with the plain language of the CFAA, and given the care with which we must interpret criminal statutes to ensure that defendants are on notice as to which acts are criminal, we decline to adopt the interpretation of "without authorization" suggested by *Citrin*. Rather, we hold that a person uses a computer "without authorization" under β 1030(a)(2) and (4) when the person has not [**21] received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.

Based on this plain-language interpretation of the CFAA, we must consider whether Brekka acted "without authorization" when he emailed LVRC documents from his work computer to himself and to his wife. There is no dispute that Brekka was given permission to

use LVRC's computer and that he accessed documents or information to which he was entitled by virtue of his employment with LVRC. Because Brekka had authorization to use the LVRC computer, he did not access a computer "without authorization." Therefore, the district court did not err in holding that LVRC failed to raise a genuine issue of material fact with respect to LVRC's claim that Brekka violated β 1030(a)(2) and (4) while he was still employed by LVRC.⁷

7 On appeal, LVRC argues only that Brekka was "without authorization" to access LVRC's computer and documents. To the extent LVRC implicitly argues that Brekka's emailing of documents to himself and to his wife violated β 1030(a)(2) [**22] and (4) because the document transfer "exceed[ed] authorized access," such an argument also fails. As stated by the district court, it is undisputed that Brekka was entitled to obtain the documents at issue. Moreover, nothing in the CFAA suggests that a defendant's authorization to obtain information stored in a company computer is "exceeded" if the defendant breaches a state law duty of loyalty to an employer, and we decline to read such a meaning into the statute for the reasons explained above. Accordingly, Brekka did not "obtain or alter information in the computer that the accesser is not entitled so to obtain or alter," *see* 18 U.S.C. β 1030(e)(6), and therefore did not "exceed [] authorized access" for purposes of β 1030(a)(2) and (4).

[*1136] IV

We next consider whether the district court erred in holding that LVRC did not raise a genuine issue of material fact with respect to its claim that Brekka violated the CFAA by logging into the LOAD website after he left LVRC. There is no dispute that if Brekka ac-

cessed LVRC's information on the LOAD website after he left the company in September 2003, Brekka would have accessed a protected computer "without authorization" for purposes of the [**23] CFAA.

LVRC argues that there was sufficient evidence to create a genuine issue of material fact as to whether Brekka was responsible for the "cbrekka" log-in on November 19, 2004 to the LOAD website and also as to whether he accessed the website on numerous other occasions after he left LVRC. We disagree.

First, LVRC claims that no LVRC employee except Brekka had knowledge of the "cbrekka" log-in. Brekka, however, provided undisputed evidence that he left the email containing the administrative user name and password on his computer when he left LVRC, that at least two LVRC employees used the computer, and that others had access to the computer after Brekka left the company. Although LVRC points to evidence that the email with the log-in information was deleted from Brekka's LVRC computer, the district court correctly determined that the record does not indicate when the log-in information was deleted. While we must draw all reasonable inferences in favor of the non-moving party, we need not draw inferences that are based solely on speculation. *See Lakeside-Scott v. Multnomah County*, 556 F.3d 797, 802-03 (9th Cir. 2009); *see also Lujan v. Nat'l Wilderness Fed'n*, 497 U.S. 871, 888, 110 S. Ct. 3177, 111 L. Ed. 2d 695 (1990) [**24] (holding that the summary judgment standard does not require that all ambiguities in the evidence be resolved in favor of the non-moving party). On appeal, LVRC relies on a declaration by its computer expert stating that the computer was reformatted before the other employees used it. However, this declaration was not part of the record before the district court on summary judgment, and therefore we do not consider it. *See Forsberg v. Pac. Nw. Bell Tel. Co.*, 840 F.2d 1409, 1417-18 (9th Cir. 1988).

Second, LVRC argues that because the computer that logged into the LVRC website on November 19 was connected to an ISP in Redwood City, a city located in Northern California, and Brekka was attending a meeting in San Francisco, which is also in Northern California, a reasonable juror could infer that Brekka was the person who accessed the website. But Brekka put forth an expert who stated that the information regarding Redwood City was related to the location of the ISP server, and did not indicate the location of the person using the "cbrekka" log-in. Jones, LVRC's witness, testified that he did not know where the person logging into the computer was located. No other evidence supported the [**25] inference that Brekka used the Redwood City ISP. Accordingly, evidence of the ISP's location is insufficient to create a genuine issue of material fact that Brekka was the person logging into the LVRC website. *See Lujan*, 497 U.S. at 888 (refusing to draw inferences in favor of the non-moving party that were not supported with specific evidence).

Finally, in connection with its action against Brekka, LVRC retained a computer expert who examined Brekka's personal computers. The expert's report stated that Brekka's personal computer had been [**1137] used to access reports and statistics from LOAD at various times, including on September 17, 2005. LVRC argues that this report indicates that Brekka logged into the LOAD website after he left LVRC's employ.

This argument also fails. As the district court noted, the expert's evidence that Brekka logged into the site on September 17, 2005 was contradicted by Nick Jones's testimony that, upon Greenstein's request, he deactivated the "cbrekka" user name and password no later than November 19, 2004. In its response to the motion for summary judgment, LVRC did not provide any explanation, let alone supporting evidence, to show how the log-in could have been [**26] used nearly a year after LVRC's

own witness testified that it had been deactivated. "If the factual context makes the non-moving party's claim of a disputed fact implausible, then that party must come forward with more persuasive evidence than otherwise would be necessary to show that there is a genuine issue for trial." *Blue Ridge Ins. Co. v. Stanewich*, 142 F.3d 1145, 1147 (9th Cir. 1998). With no explanation or evidence as to how Brekka would have used the "cbrekka" log-in to access the LOAD website after the log-in was deactivated, we cannot say that there was a genuine issue of material fact regarding whether Brekka logged into the LOAD website after he left LVRC. The district court did not err when it refused to resolve the ambiguities in LVRC's own evidence in favor of LVRC.

On appeal, LVRC argues for the first time that it subsequently reactivated the "cbrekka" user name to help LVRC catch and identify the person who was misusing the log-in. LVRC points to an FBI report in the record that contains a statement from an unknown person to this effect. The FBI report was submitted as part of the summary judgment motion in Brekka's third-party suit, but LVRC did not draw the district [**27] court's attention to this statement regarding the reactivation of the "cbrekka" log-in in its response to the motion for summary judgment in this case, or even refer to the reactivation of the log-in in any of its filings. We will not reverse a district court's grant of summary judgment unless the party

opposing the summary judgment motion has identified the evidence establishing a genuine issue of material fact in its opposition to summary judgment. *See Carmen v. San Francisco Unified School District*, 237 F.3d 1026, 1031 (9th Cir. 2001). Because LVRC failed to do so in this case, we do not consider LVRC's proffered evidence that the "cbrekka" log-in was reactivated in November 2004.

Because LVRC did not meet its burden of producing "evidence that is significantly probative or more than 'merely colorable' that a genuine issue of material fact exists for trial," *FTC v. Gill*, 265 F.3d 944, 954 (9th Cir. 2001) (quoting *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 249-50, 106 S. Ct. 2505, 91 L. Ed. 2d 202 (1986)), the district court did not err in granting summary judgment in favor of Brekka.

V

Brekka's use of LVRC's computers to email documents to his own personal computer did not violate β 1030(a)(2) or β 1030(a)(4) because [**28] Brekka was authorized to access the LVRC computers during his employment with LVRC. Moreover, construing the evidence in the record before the district court in the light most favorable to LVRC, there is not enough evidence upon which a reasonable jury could find that Brekka violated the CFAA after he left the company.

AFFIRMED.