[PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 19-11100

D.C. Docket No. 8:17-cv-00472-WFJ-SPF

PERI DOMANTE,

Plaintiff-Appellant,

versus

DISH NETWORKS, L.L.C.,

Defendant-Appellee.

Appeal from the United States District Court
for the Middle District of Florida

(September 9, 2020)

Before BRANCH, LUCK, and ED CARNES, Circuit Judges.

PER CURIAM:

Peri Domante appeals the district court's grant of summary judgment in favor of Dish Networks in Domante's civil suit for breach of contract and violations of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681b. This dispute arose after Dish requested and obtained Domante's consumer report from a consumer reporting agency after an identity thief fraudulently submitted some of Domante's personal information to Dish. Despite the fact that Dish discovered the fraud after receiving the report and never opened an account in Domante's name, Domante alleges that Dish negligently and willfully violated the FCRA simply by requesting and obtaining the consumer report in the first place. Domante also alleges that Dish's actions violated a settlement agreement that the parties signed after a similar incident occurred several years ago involving the same parties. In that agreement, Dish promised to flag Domante's social security number to prevent future fraudulent attempts to obtain Dish services in Domante's name. After the benefit of oral argument and careful review, we affirm the district court, holding that Dish had a "legitimate business purpose" under the FCRA when it obtained Domante's consumer report and that Dish did not violate the settlement agreement.

I. Background

In both 2011 and 2013, Domante was a victim of identity theft, as her personal information was stolen and used fraudulently to open two accounts with

Dish, a provider of television services. Domante was alerted to the fraud after the accounts became delinquent, and she then sued Dish and Equifax Information Services, LLC, alleging non-compliance with the FCRA. Domante and Dish ultimately entered a settlement agreement in October 2016. Pursuant to the terms of the settlement agreement, Domante agreed to dismiss her claims against Dish in exchange for Dish's promise "to flag [Domante's] social security number in order to preclude any persons from attempting to obtain new [Dish] services by utilizing [Domante's] social security number." To comply with the settlement agreement, Dish input Domante's personal information—first name, last name, date of birth, and full social security number—into one of its internal mechanisms meant to flag and prevent unauthorized accounts from being opened.

Individuals can apply for Dish services in a variety of ways, including online and over the phone. An online applicant provides only the last four digits of his or her social security number. To verify the online applicant's identity and eligibility for services, Dish's system automatically sends the applicant's information to a consumer reporting agency.[1] If the consumer reporting agency determines it has a

[1] *See* 15 U.S.C. § 1681a(f) (defining "consumer reporting agency" as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports").

match to the submitted information, it provides a "consumer report"[2] to Dish containing the applicant's full social security number. Once Dish receives the full social security number, it then cross-references that number using its internal mechanisms to ensure the applicant is otherwise eligible to obtain services.

On January 12, 2017, an unknown individual applied online for a Dish account using the last four digits of Domante's social security information, Domante's date of birth, and Domante's first name. However, the online applicant used a different last name, address, and telephone number. Dish's automated system submitted the applicant's information to a consumer reporting agency (in this case, Equifax) to verify the individual's identity. Equifax matched this information with Domante and returned to Dish her consumer report, which included Domante's full social security number. Dish then blocked the application from going forward, and a Dish account in Domante's name was not opened. After learning that Domante's credit report reflected that the credit inquiry had occurred, Dish requested that Equifax delete the inquiry from Domante's credit record, and Equifax obliged.

[2] Below and on appeal, Dish maintains that the social security number it obtained from the consumer reporting agency was not a "consumer report" as defined by the FCRA. *See* 15 U.S.C. § 1681a(d). We need not address that issue because we find that, assuming *arguendo* that Dish obtained a consumer report, it did so with a "permissible purpose."

Domante filed the underlying complaint in February 2017. In Counts I and II, respectively, she alleged that Dish negligently and willfully obtained the January 2017 consumer report without a "permissible purpose" in violation of § 1681b of the FCRA. In Count III, Domante alleged that Dish materially breached its contractual obligations under the settlement agreement by "requesting and obtaining [her] credit report [from Equifax], despite explicitly agreeing to flag [her] social security number so as to prevent any person from opening an account with [Dish] using [her] social security number." Domante sought actual, statutory, and punitive damages, injunctive relief, and attorney's fees.[3]

During the pendency of the instant litigation, on January 23, 2018, yet another online application was submitted to Dish by an unknown individual using only the last four digits of Domante's social security number and correct first name. As before, Dish requested a consumer report from Equifax, received from Equifax Domante's full social security number, cross-checked the full social security number in its internal mechanism, identified that the social security number belonged to Domante, stopped the application before an account was opened, and requested that Equifax remove the inquiry from Domante's credit report history—all by January 29, 2018. That *very* day, yet another fraudulent attempt was made to open a Dish account online using Domante's information.

[3] The sole actual damages sought by Domante were non-economic, emotional damages.

This time, however, pursuant to Dish's policy, it did not request a consumer report because the application was submitted within a 90-day window of a previously denied application using the same information. Thus, Dish prevented both fraudulent online attempts in January 2018 from ripening into a Dish account in Domante's name.

Upon cross motions for summary judgment,[4] the district court ruled in favor of Dish on all three counts. Regarding Domante's claims for negligent and willful non-compliance with the FCRA, the district court found that Dish had a "legitimate business need" to verify the identity and determine the eligibility of the online applicant when it obtained a consumer report from Equifax in January 2017.[5] The district court also found that Domante's breach of contract claim failed because Dish satisfied its contractual obligations by "flagging" Domante's full social security number and preventing an account from being opened in her name.[6] Domante timely appealed.

---

[4] Dish moved for summary judgment on all three counts. Domante moved for summary judgment on her FCRA claims and partial summary judgment as to liability on her breach of contract claim.

[5] The district court noted that the instances of fraud on January 23 and 29 of 2018 were not included in Domante's complaint, but that even if they were, those two instances are "insufficient to alter the Court's analysis" as to either the § 1681b or breach of contract claims. We agree.

[6] The district court also stated that Domante was "potentially" precluded from relief under the FCRA because she could not demonstrate that she had suffered damages. We need not address the issue of damages because we agree that Dish did not violate the FCRA by making its January 2017 inquiry to the consumer reporting agency.

II. Standard of Review

We review *de novo* a district court's order on cross motions for summary judgment. *Owen v. I.C. Sys., Inc.*, 629 F.3d 1263, 1270 (11th Cir. 2011). Summary judgment is appropriate when there is "no genuine dispute as to any material fact" and the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(a). We view the evidence and draw all reasonable inferences in the light most favorable to the non-moving party. *Owen*, 629 F.3d at 1270.

III. Discussion

A. FCRA Claims

The district court did not err by ruling in favor of Dish on the FCRA claims. The FCRA enumerates an exhaustive list of the "permissible purposes" for which a person[7] may use or obtain a consumer report. 15 U.S.C. § 1681b(a)(3); *id.* § 1681b(f)(1); *see Pinson v. JP Morgan Chase Bank, Nat'l Ass'n*, 942 F.3d 1200, 1213 (11th Cir. 2019). One of those permissible purposes is where a person "has a *legitimate business need* for the information . . . in connection with a business transaction that is initiated by the consumer." 15 U.S.C. § 1681b(a)(3)(F)(i) (emphasis added).

We have never weighed in on what constitutes a "legitimate business need" in connection to a business transaction for FCRA purposes. The Sixth Circuit,

[7] In this case, the "person" obtaining the consumer report is Dish.

however, has addressed the meaning of "legitimate business need" in a situation very similar to the one here—in fact, it involved the same defendant. *See Bickley v. Dish Network, LLC*, 751 F.3d 724 (6th Cir. 2014). In *Bickley*, the plaintiff argued in part that Dish violated § 1681b when Dish requested and used his credit report after receiving an application for Dish services by phone, despite the fact that Dish had prevented an identity theft in so doing. *Id.* at 726, 732. The Sixth Circuit disagreed that Dish had violated the FCRA and affirmed the district court's grant of summary judgment to Dish on those claims. In so doing, the court held that the term "legitimate business need" in § 1681b includes "verifying the identity of a consumer and assessing his eligibility for a service." *Id.* at 731; *accord Estiverne v. Sak's Fifth Ave.*, 9 F.3d 1171, 1173 (5th Cir. 1993) (holding that a retail store had a "legitimate business need" under the FCRA when it requested a credit report to determine whether to accept or reject a consumer's check).

Similar to its winning argument in *Bickley*, here Dish contends that it requested and obtained Domante's consumer report from Equifax in an effort to verify the identity and determine the eligibility of the potential consumer who applied online for Dish services in January 2017 and, in so doing, prevented an identity theft. The district court found that verification for eligibility indeed was Dish's purpose in requesting and obtaining the report. We see no genuine factual dispute, as Dish clearly relied on Equifax for this purpose whenever an individual

applied for Dish services online. And we agree with the Sixth Circuit that requesting and obtaining a consumer report for verification and eligibility purposes is a "legitimate business need" under the FCRA. *See id.* at 731; *see also Estiverne*, 9 F.3d at 1173. Thus, Dish had a permissible purpose in obtaining Domante's consumer report and did not run afoul of § 1681b by doing so.

Arguing to the contrary, Domante contends that Dish did not have a legitimate business need because Dish either knew or should have known that Domante had not initiated the business transaction because of their prior settlement agreement. We find this argument unpersuasive. Like the plaintiff in *Bickley*, Domante "blithely ignores that a consumer did initiate the transaction." *Bickley*, 751 F.3d at 732. [8] When the unknown applicant applied for Dish services online in January 2017, Dish had only the last four digits of the provided social security number, not the full number. Dish depended in part on Equifax's consumer-report services to verify the identity of the applicant so that it could obtain the full social security number and cross-check that information via its internal mechanisms. And, contrary to Domante's assertions, the fact that *Equifax* had the mechanisms in place to verify that the scant information provided by the January 2017 applicant

[8] Domante asserts that *Bickley* is distinguishable because there, unlike here, Dish had no prior dealings with the plaintiff. But even assuming that such prior dealings are relevant generally, they do not matter in this case because Domante cannot show that Dish affirmatively knew the fraudulent application contained her personal information at the time it requested the consumer report.

actually belonged to Domante does not necessarily lead to the conclusion that *Dish* suspected (or was able to verify) the same.

Although Domante suggests that Dish should have done more to verify her identity before requesting a consumer report, the FCRA does not explicitly require a user of consumer reports to confirm beyond doubt the identity of potential consumers before requesting a report. We are not at liberty to add statutory language where it does not exist. *See Bostock v. Clayton Cty., Ga.*, 140 S. Ct. 1731, 1823 (2020) (Kavanaugh, J., dissenting) ("[W]e are judges, not Members of Congress. . . . Under the Constitution's separation of powers, our role as judges is to interpret and follow the law as written, regardless of whether we like the result. . . . Our role is not to make or amend the law."); *Harris v. Garner*, 216 F.3d 970, 976 (11th Cir. 2000) ("[T]he role of the judicial branch is to apply statutory language, not to rewrite it.").

Domante also argues that the settlement agreement itself established that Dish did not have a legitimate business need to access her credit report. Specifically, Domante argues that because the agreement precluded any Dish account from being opened in her name, even by Domante herself, there was no legitimate business need to obtain her credit report. Domante's argument about contracting around the FCRA fails, however. As discussed above, at the time Dish requested a consumer report for the fraudulent online application, Dish did not yet

have enough information to connect the online application to Domante. Rather, all the online application provided to Dish was a partial identity—a first name, birth date, and last four digits of a social security number. True, this limited information matched Domante. But the settlement agreement does not expressly prohibit Dish from entertaining an application from a potential consumer who happens to share a few personal identifiers with Domante.

We therefore affirm the district court's holding that Dish did not violate § 1681b because Dish had a legitimate business need, and thus a permissible purpose, for obtaining the consumer report in January 2017.

B. Breach of Contract

Domante next contends that Dish breached the settlement agreement. In relevant part, the settlement agreement provided that

> [Dish] agrees to flag [Domante's] social security number in order to preclude any persons from attempting to obtain new [Dish] services by utilizing [Domante's] social security number.

Based on this language, Domante argues that Dish agreed to preclude any external credit inquiry involving her information following the attempted fraudulent transaction. Thus, she maintains that Dish violated the settlement agreement when it made the January 2017 credit inquiry.

Under Florida law, a plaintiff asserting a breach of contract claim must demonstrate "(1) the existence of a contract, (2) a breach of the contract, and

(3) damages resulting from the breach." *Rollins, Inc. v. Butland*, 951 So. 2d 860, 876 (Fla. 2d Dist. Ct. App. 2006). The district court found that Domante's claim failed to establish the breach element.[9] We agree.

The only affirmative action Dish agreed to take in the settlement agreement was "to flag" Domante's "social security number." As an initial matter, Dish satisfied that contract term when, after entering into the settlement agreement, it input Domante's personal information—first name, last name, date of birth, and full social security number—into one of its internal mechanisms as a "flag." And Dish again satisfied the terms of the agreement when, after obtaining Domante's full social security number from Equifax following the January 2017 online application, it plugged the number into its internal system, triggered the "flag," and stopped the fraudulent application without opening an account. Thus, Dish did not breach the settlement agreement, and Domante's arguments to the contrary fail.

IV. Conclusion

For the foregoing reasons, summary judgment in favor of Dish was appropriate.

AFFIRMED.

[9] As to the claim for breach of the settlement agreement, the district court expressly declined to reach the issue of damages. We too find it unnecessary to reach that issue.