UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

PERI DOMANTE,

Plaintiff,

v. Case No. 8:17-cv-00472-T-02SPF

DISH NETWORKS, LLC.,

Defendant.
_____/

ORDER

This action concerns the production of a consumer report following an unfortunate case of identity theft. The matter comes to the Court on cross-motions for summary judgment from Plaintiff Domante and Defendant Dish Networks, LLC. Dkts. S-147, S-149. The parties have responded to the opposing motions. Dkts. S-162, S-164. The Court took extensive oral argument on the motions. The Court DENIES Plaintiff's Amended Motion for Partial Summary Judgment as to Liability, Dkt. S-147, and GRANTS Defendant's Amended Motion for Final Summary Judgment, Dkt. S-149. The motions in limine are denied as moot.

BACKGROUND

The background facts of this case are, in all material respects, undisputed. Unknown individuals used Plaintiff's personal information, including her social security number, to open fraudulent accounts with Defendant, a provider of television services. Dkt. 166 at 12. Plaintiff sued Defendant and Equifax Information Services, LLC (Equifax) under the Fair Credit Reporting Act (FCRA) over a dispute involving credit reporting related to the accounts. *Id.* Plaintiff eventually dismissed the case against Defendant pursuant to a settlement agreement. *Id.* According to the agreement, "[i]n full consideration for the releases, covenants and other terms and conditions provided herein, DISH agrees to flag Plaintiff's social security number in order to preclude any persons from attempting to obtain new DISH services by utilizing Plaintiff's social security number." *Id.*

Prospective customers for services with Defendant can apply or inquire about their eligibility in various ways, including an online form on Defendant's website. *Id.* at 15; Dkt. S-147-1 at 12. The form requires individuals to input their first and last name, full address, phone number, birthday month and day, credit card information, and the last four digits of their social security number. Dkt. 166 at 13. The automated system has "scrubs" to block applications, including the grimly named Master Death List (MDL), a Pre-Qual customer check, a

grandfathered customer check, a social security overuse check, and a credit card authorization check. *Id.*; Dkt. S-147-1 at 31-32.

The MDL is an internal catalog of social security numbers provided by the Social Security Administration that belong to deceased individuals. Dkt. 166 at 7 n.3. Defendant cross-checks the social security number of each application for services against the MDL to ensure the number belongs to a living person. *Id.* Defendant runs this "deceased check" at both the beginning of the application process if it has the full social security number and after a credit inquiry when a full and accurate social security number has been returned. *Id.* The grandfathered customer check prevents duplicate applications with the same social security number, date of birth, and zip code information within ninety days. *Id.* at 15. The system will transmit to Defendant's credit reporting agencies (CRAs), including Equifax, information included on applications that pass all the above checks. Dkt. S-147-1 at 15.

To satisfy its obligation under the settlement agreement with Plaintiff, Defendant decided to add Plaintiff's information, including her full social security number, on the MDL. Dkt. 166 at 13; Dkt. S-147-1 at 41. Shannon Picchione, Defendant's Vice President, testified that this is the only instance Defendant has done this. Dkt. S-147-1 at 42. Notwithstanding this measure, on January 12, 2017 an unidentified individual submitted an online application through Defendant's

website for DISH services using the last four digits of Plaintiff's social security number, Plaintiff's first name, and a different last name, address, and telephone number than that of the Plaintiff. Dkt. 166 at 14. Defendant's automated system forwarded this application to Equifax. *Id.*; Dkt. S-147-1 at 49. Based on the information, Equifax returned to Defendant a credit report for Plaintiff. Dkt. 166 at 14; Dkt. S-147-1 at 49. The matter then ended as Plaintiff's full social security number was blocked by Defendant's MDL. Dkt. S-147-1 at 49. However, this activity triggered a credit inquiry notation shown on Plaintiff's credit report that, according to Defendant, was removed on April 5, 2017. Dkt. 166 at 14.

On February 24, 2017, Plaintiff sued Defendant for negligent and willful noncompliance with § 1681b of the FCRA and breach of contract. Dkt. 1 at 5-12. She alleges that, as a result of the January 2017 events, Defendant obtained a consumer report from Equifax with Plaintiff's information without a permissible purpose in violation of the FCRA. *Id.* ¶¶ 35, 36, 52, 53. She further alleges Defendant materially breached the settlement agreement by "requesting and obtaining [Plaintiff's] credit report maintained by [Equifax] despite explicitly agreeing to flag [Plaintiff's] social security number so as to prevent any person from opening an account with Defendant using [Plaintiff's] social security number." *Id.* ¶ 68. She seeks actual, statutory, and punitive damages, attorney's

fees, and injunctive relief. *Id.* at 7, 10-11. Plaintiff's sole actual damages are non-economic, *i.e.* vexation damages.

On January 23, 2018, after the filing of the lawsuit, an unidentified individual again submitted an online application through Defendant's website for DISH services using the last four digits of Plaintiff's social security number, Plaintiff's first name, and a different last name, address, and telephone number than that of the Plaintiff. Dkt. 166 at 14. This triggered a credit inquiry that, according to Defendant, was removed by January 29, 2018. *Id.* On the same day, another application was submitted with the same social security number, date of birth, and zip code as in the January 23, 2018 application. *Id.* at 15. This duplicate application triggered the grandfather check at DISH, which prevented a credit inquiry from going to Equifax from DISH. *Id.* These latter two (2018) instances are not explicitly mentioned in Plaintiff's Complaint. Plaintiff was unaware of them until discovery was produced by Defendant.

The Court denied Defendant's earlier motion to dismiss, noting that summary judgment would be a more appropriate stage to evaluate the claims. Dkt. 37 at 3-5. The parties have developed a full record and argued ably both in their briefing and at oral argument. The matter is now ripe for consideration.

SUMMARY JUDGMENT STANDARD

Under Rule 56, Federal Rules of Civil Procedure, "[t]he court shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a); *see also Mize v. Jefferson City Bd. of Educ.*, 93 F. 3d 739, 742 (11th Cir. 1996). If met, the burden shifts to the nonmoving party to "come forward with specific facts showing that there is a genuine issue for trial." *Shaw v. City of Selma*, 884 F. 3d 1093, 1098 (11th Cir. 2018) (citation omitted).

"A fact is 'material' if it has the potential of 'affect[ing] the outcome of the case.'" *Shaw*, 884 F.3d at 1098. "And to raise a 'genuine' dispute, the nonmovant must point to enough evidence that 'a reasonable jury could return a verdict for [him].'" *Id.* (citation omitted) (modification in original). The Eleventh Circuit further teaches that "[w]hen considering the record on summary judgment 'the evidence of the nonmovant is to be believed, and all justifiable inferences are to be drawn in his favor.'" *Id.* (citations omitted).

DISCUSSION

The Court finds that Defendant did not violate the FCRA or the settlement agreement. Summary judgment in favor of Defendant is therefore appropriate.

I. Defendant did not violate the FCRA.

An FCRA claim requires a plaintiff to prove: "(i) that there was a consumer report[1], (ii) that defendants used or obtained it, (iii) that they did so without a permissible statutory purpose, and (iv) that they acted with the specified culpable mental state." *Jimenez v. Account Servs.*, 233 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017) (citations omitted). One such permissible purpose is that a CRA may furnish a consumer report "[t]o a person which it has reason to believe . . . 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). Courts have also applied this "'reasonable belief' standard to . . . users of consumer reports to determine whether their reasons for . . . acquiring the reports are permissible." *Glanton v. DirecTV, LLC*, 172 F. Supp. 3d 890, 896 (D.S.C. 2016) (collecting cases).[2]

Boiled down, Plaintiff argues that Defendant had no permissible purpose in obtaining Plaintiff's consumer report from Equifax because Defendant should have known that it was some third party online, and not Plaintiff who queried

[1] Defendant seems to object to the characterization of the information received from Equifax as a "consumer report." Dkt. S-165 at 20. The Court need not resolve this question in finding no violation of the FCRA.

[2] As for liability, the FCRA provides that an entity that is willful or negligent in failing to comply with a requirement with "respect to any consumer is liable to that consumer . . . ." §§ 1681o, 1681n(a). Willful conduct includes conduct in "reckless disregard of a consumer's rights under the FCRA." *Rambarran v. Bank of Am., N.A.*, 609 F. Supp. 2d 1253, 1270 (S.D. Fla. 2009) (citations and quotation marks omitted).

eligibility for Defendant's services. Put differently, Defendant should have flagged Plaintiff's information in such a way that Defendant's automated system would not allow even a credit inquiry to a CRA.

Just as the Court looked to *Bickley v. Dish Network, LLC*, 751 F.3d 724 (6th Cir. 2014) at the motion to dismiss stage, so too is the case instructive here. There, an identity thief or third party sought services in Bickley's name. *Id.* at 726. The court began by noting that it is "clear that a company has a 'legitimate business need' when it assesses a consumer's *eligibility* for a business service." *Id.* at 731 (citation omitted) (emphasis in original). Indeed, this very process "protects innocent consumers . . . whose identity might otherwise be stolen." *Id.* The court further rejected the plaintiff's argument that he did not "initiate" the business transaction, observing that:

> [The plaintiff] is suggesting that [the defendant] violated the statute when it attempted to verify that it was in compliance with the statute by ensuring that the transaction had in fact been initiated by the consumer. This cannot be accurate, which is perhaps why there is, unsurprisingly, *no* case law to support the position. The requirement that a consumer "initiate" a business transaction is designed to protect a consumer's privacy and credit-related data by preventing companies from running credit checks that are unrequested by the consumer. It is readily apparent that such malfeasance did not occur in the present case. To the contrary, by executing a cross-verification process, [the defendant] safeguarded the integrity of [the plaintiff's] data and identity.

Id. at 732 (emphasis in original); *see also Glanton*, 172 F. Supp. 3d at 896 ("Courts have reached the conclusion that there is no violation of Section 1681b when a creditor obtains a credit report due to an imposter's application for credit even though the identity theft victim did not make the application.").[3]

Crucial to *Bickley*'s holding, Plaintiff suggests, was the defendant's belief that the plaintiff was a potential customer and that the defendant's attempt to verify the consumer's identity and eligibility was in good faith. *Id.* at 732. Plaintiff further argues that, unlike this case, *Bickley* did not involve a history of prior fraudulent activity that might undercut such a finding. Yet the facts presented here, apparently a novel extension of *Bickley* and *Glanton*, do not stray so far as to compel a different result.

Assuming for the moment that the prior instances put Defendant on notice of the danger of fraudulent inquiries with Plaintiff's information—or even that the settlement agreement somehow modified Defendant's obligations under the FCRA—the question is still the same: was there a legitimate business need in connection with a business transaction initiated by the consumer? Indeed,

[3] The cases Plaintiff relies upon outside of the identity theft context are unpersuasive. And a case like *Rand v. Citibank, N.A.*, No. 14-CV-04772 NC, 2015 WL 510967 (N.D. Cal. Feb. 6, 2015) is readily distinguishable because the defendant there "knew or should have known" that the plaintiff was not involved with a credit application where he was a longtime customer of the defendant's and the social security number was incorrect. *Id.* at *3; *see also Cappetta v. GC Servs. Ltd. P'ship*, 654 F. Supp. 2d 453, 461 (E.D. Va. 2009) (denying motion to dismiss where allegations included that "[a]t the time [the defendant] obtained the Plaintiff's consumer report . . . the Defendant *knew* it was not in possession of any application on the account and that Plaintiff was only listed, at most, as a supplemental cardholder on the account").

Defendant had a legitimate business need to verify the identity and eligibility of the individual who applied for Defendant's services on January 12, 2017. Furthermore, the factual record simply does not support the assertion that Defendant did not reasonably or in good faith believe the individual was not who he said he was.[4] This is especially so when the third party (no doubt intentionally) alters the inputted information.

Plaintiff puts forth alternatives for Defendant to satisfy its contractual—and for the sake of argument, statutory—obligation to "flag" Plaintiff's social security number, but each is flawed. For example, flagging only the last four, non-unique digits of Plaintiff's number would potentially result in a multitude of false hits on the MDL. Dkt. S-147-1 at 31. Even combining the four digits with Plaintiff's date of birth or last name could generate multiple hits. *Id.* at 52. Equally unavailing is flagging other identifying information, such as a zip code, which can be spoofed as happened here with Plaintiff's last name and other data. It is, moreover, not possible to create a fake account to prevent a credit inquiry. *Id.* at 50.

To be sure, it is feasible for Defendant to require all nine digits of a social security number for an online application as it does with applications over the telephone. *Id.* at 14. Or perhaps Defendant could rework the grandfather filter to

[4] The January 23 and 29, 2018 instances are not explicitly included in Plaintiff's Complaint. Even assuming the broadly worded Complaint successfully pleaded the future activity, the two instances are insufficient to alter the Court's analysis as either discrete violations of § 1681b or as to the finding of Defendant's reasonable belief.

catch applications with Plaintiff's information.[5] Plaintiff observes that Defendant's objections to these or other alternatives is a business, if not technical, decision. *See id.* at 52. But Plaintiff does not challenge Defendant's online application process as itself violative of the FCRA—merely that some additional data was required to be checked or collected from a potential customer before seeking to verify the applicant through Defendant's CRAs.

The events giving rise to litigation belie this contention. Defendant decided that the MDL was an effective "flag" of Plaintiff's information that prevented the opening of fraudulent accounts. On January 12, 2017, an unknown individual used Plaintiff's personal information to apply for services with Defendant. Thanks to Defendant's credit inquiry, Defendant discovered that the individual was not Plaintiff and immediately stopped the application. No application was approved, no account was opened, and the credit inquiry was removed from Plaintiff's credit report once Defendant discovered it.

This satisfies Defendant's obligations under the FCRA. There is no genuine dispute as to a material fact, and judgment for Defendant is appropriate on the FCRA claims.

[5] At oral argument, Plaintiff stressed that Defendant had the capability to use the grandfather check, which prevented an inquiry following the January 29, 2018 duplicate application, to stop the January 12, 2017 application. But the grandfather check requires duplicate information within a ninety-day period, so clearly some unspecified manipulation would be required. *See* Dkt. S-147-1 at 50.

II. Damages

An alternate ground that potentially precludes relief is the absence of damages. Though in her Complaint Plaintiff alleges suffering of at least four years, mental distress and emotional anguish, a "waste of time," a negative impact to her credit worthiness, and an increase of her cost of credit, Dkt. 1 at 6-7, the evidence did not bear this out. At most, Plaintiff has lost sleep and suffers some anxiety and stress. Dkt. S-147-2 at 26, 35; Dkt. S-147-4 at 42-43. Yet the connection of any damages to Defendant's alleged violations is tenuous, especially since Defendant prevented the opening of any accounts and the January 12, 2017 credit inquiry was on Plaintiff's consumer report only briefly. Though the Court is sympathetic to the stress that the ordeal has caused, its major source is the actions of the unknown third party, not Defendant.

Moreover, apart from the marginal cost of using credit monitoring services, Plaintiff is unable to cite any economic damages. She has not, for example, seen a physician for her anxiety, Dkt. S-147-2 at 26, nor is there any indication she has been denied credit, a favorable rate, or a loan because of the credit inquiries on her consumer report, Dkt. 166 at 16.

In any event, because Defendant had a permissible purpose in obtaining Plaintiff's consumer report from Equifax, the Court need not determine whether the absence of a certain type of damages would otherwise preclude relief for at

least some of the claims. *See, e.g., Taylor v. Screening Reports, Inc.*, 294 F.R.D. 680, 686 (N.D. Ga. 2013) (citations omitted) ("To prove a case of negligent noncompliance, Plaintiff must produce some evidence of actual damages caused by the violation."). Nor need the Court measure the extent to which damages might be compensable. *See Levine v. World Fin. Network Nat. Bank*, 437 F.3d 1118, 1125 (11th Cir. 2006) (leaving open "whether FCRA bars recovery for any particular category of compensatory damages, including emotional distress, and the extent to which the common law informs this analysis"); *see also Collins v. Experian Info. Sols., Inc.*, 775 F.3d 1330, 1335 (11th Cir. 2015) (remanding case for district court to determine whether "evidence of emotional distress was sufficient to present a jury question on actual damages"); *Brim v. Midland Credit Mgmt., Inc.*, 795 F. Supp. 2d 1255, 1260 (N.D. Ala. 2011) ("The Eleventh Circuit has never precisely delineated the factors that a court should consider in determining whether the plaintiff's evidence of emotional distress [from an FCRA violation] is sufficient to support the jury's award of compensatory damages for emotional distress, particularly where, as here, the plaintiff's damages evidence consists chiefly of his own testimony.").

III. Defendant did not breach the settlement agreement.

Plaintiff's breach of contract claim similarly fails. The settlement agreement stemming from the prior action provides that, "[i]n full consideration for the

releases, covenants and other terms and conditions provided herein, DISH agrees to flag Plaintiff's social security number in order to preclude any persons from attempting to obtain new DISH services by utilizing Plaintiff's social security number." Breach of contract requires "(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 DCA 2006) (citations omitted). The Court finds there was no breach.[6]

Though sparse in content, the language of the contract is unambiguous and clear on its face. *See Charbonier Food Servs., LLC v. 121 Alhambra Tower, LLC*, 206 So. 3d 755, 758 (Fla. 3d DCA 2016) (citation omitted) ("Where a contract is unambiguous, it shall be enforced according to its plain language."). Plaintiff's obligation under the contract is to "flag Plaintiff's social security number." The purpose is to "preclude any persons from attempting to obtain new DISH services by utilizing Plaintiff's social security number." Indeed, Defendant did flag the number—which is to say, the nine-digit combination of numbers that constitutes a person's social security number—by listing it, along with other identifying information, on the MDL.[7]

[6] As with the FCRA claims, the Court need not reach the question of damages for either establishing liability or appropriate relief.

[7] Ms. Picchione testified that "flag" does not have any special meaning in Defendant's operations. She interpreted the term to mean simply "identifying." Dkt. S-147-1 at 28.

Importantly, in no way did Defendant agree to stop any third party from using Plaintiff's information to apply for services. Even looking beyond the contract's plain language, to read "attempting" as Plaintiff suggests would impose upon Defendant a virtually impossible burden. Defendant would arguably breach the contract if a third party merely inputted Plaintiff's personal information on Defendant's online application page. Plaintiff admits, as she must, she does not believe Defendant has any power to prevent a third party such as a hacker from inputting her information online. Dkt. S-147-2 at 27. Indeed, before execution of the agreement, Defendant "represented that a third party cannot be prevented from using Plaintiff's personal information to apply for credit." Dkt. 166 at 13.

In essence, Plaintiff argues that though Defendant might have flagged the social security number, the result was not to her liking. But, as explained above, the method by which Defendant satisfied its contractual duty to flag did in fact prevent the unknown third party from "obtain[ing] new DISH services by utilizing Plaintiff's social security number." Thus, not only was Plaintiff's obligation under the contract satisfied, but so too was the agreement's underlying goal. There is no genuine dispute as to any material fact on this matter, and judgment is appropriate for Defendant on the breach of contract claim.

CONCLUSION

The Court DENIES Plaintiff's Amended Motion for Partial Summary Judgment as to Liability, Dkt. S-147, and GRANTS Defendant's Amended Motion for Final Summary Judgment. Dkt. S-149. The motions in limine are denied as moot. Dkts. 96-100, 168, 169. The Clerk is directed to enter judgment accordingly, terminate any pending motions, and close the case.

DONE AND ORDERED at Tampa, Florida, on February 22, 2019.

/s/ William F. Jung
WILLIAM F. JUNG
UNITED STATES DISTRICT JUDGE

COPIES FURNISHED TO:
Counsel of Record