IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

CONSUMERDIRECT, INC.,
Plaintiff,

v.

MYFREESCORENOW.COM, INC., and
BRUCE CORNELIUS,
Defendants.

Case No. 8:2026-cv-00988

BRIEF OF AMICUS CURIAE JOEZIEL VAZQUEZ-DAVILA

Board Certified Credit Consultant (BCCC, CCSC, CCRS)
CEO & Founder, Credlocity Business Group LLC
Consumer Advocate and Investigative Journalist

IN SUPPORT OF CONSUMERDIRECT AND IN PROTECTION OF CONSUMER DATA RIGHTS

TABLE OF CONTENTS

I. IDENTITY AND INTEREST OF AMICUS CURIAE

Amicus curiae Joeziel Vazquez-Davila submits this brief pro se pursuant to the inherent authority of this Court to receive submissions from interested parties with specialized knowledge bearing on matters before it. Amicus respectfully requests leave to file this brief and asks that it be considered in connection with any pending motions, including the application for a Temporary Restraining Order and any motions pertaining to venue and jurisdiction currently before the Court.

Amicus is the founder and Chief Executive Officer of Credlocity Business Group LLC, a Philadelphia-based credit repair and consumer advocacy company established in 2007. Over seventeen years of practice, Credlocity has served in excess of 79,000 consumers navigating the credit repair process. Amicus holds Board Certified Credit Consultant (BCCC), Certified Credit Score Consultant (CCSC), and Certified Credit Repair Specialist (CCRS) credentials. Amicus has operated as an investigative journalist covering fraud, deception, and consumer harm within the credit repair industry, conducting investigations that have contributed to regulatory actions and business closures affecting bad actors in this space.

Amicus operates in the same industry ecosystem directly implicated by this litigation. The credit repair community depends on credit monitoring platforms like the one at issue here as foundational infrastructure. Amicus has direct professional knowledge of how credit repair companies and their clients use and rely on these platforms, what consumers actually understand when they enroll in them, and what the human cost of platform instability looks like in practice. That ground-level expertise is not represented by either party before this Court.

II. PRELIMINARY STATEMENT

This case presents itself to the Court as a commercial dispute between two credit monitoring companies. On its surface, it involves contract enforcement, trade secret misappropriation, and business competition. At its core, however, this litigation implicates something far more fundamental: the rights of hundreds of thousands of American consumers over their own personal financial data — data that includes Social Security numbers, full credit card information, billing histories, and credit report access credentials held by people who are, in the vast majority of cases, already financially vulnerable consumers actively working to repair their credit.

Neither party to this litigation has adequately championed the interests of those consumers. MyFreeScoreNow.com, Inc. ("MFSN") argues that the consumer data at issue belongs to MFSN by virtue of its contract with ConsumerDirect. ConsumerDirect argues it is justified in retaining that data based on security concerns about MFSN's platform. Both positions, to varying degrees, treat consumer data as a corporate asset to be leveraged in a business dispute. It is not. It never has been. Federal and California law are clear on this point.

Amicus submits this brief to address issues the parties have not raised: (1) the legal framework establishing that consumer credit data is not a corporate asset but information held in

trust; (2) the critical and widely misunderstood role that credit repair partner companies play in driving MFSN's subscriber base, and how this transition has devastated those partners and their clients; (3) the deceptive manner in which MFSN marketed its platform migration to consumers; (4) the concrete harm caused by at least three rounds of forced password resets during the transition period; and (5) why remand to California state court would better serve consumer protection interests.

III. ARGUMENT

A. CONSUMER CREDIT DATA IS NOT A CORPORATE ASSET — IT BELONGS TO THE CONSUMERS THEMSELVES

The central premise of MFSN's position in this litigation is that the consumer data at issue — including the Social Security numbers, credit card information, and financial histories of over 115,000 consumers — belongs to MFSN by virtue of Section 6.6 of the White Label Agreement. This framing fundamentally mischaracterizes the nature of consumer credit data under federal and California law.

The Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., establishes a comprehensive framework governing the collection, use, and protection of consumer credit information. The FCRA's foundational premise is that credit information exists to serve the interests of consumers, not the commercial interests of the companies that process it. See 15 U.S.C. § 1681(a)(4). The statute vests consumers with affirmative rights over their own information: the right to access it, dispute it, and control its use. 15 U.S.C. §§ 1681b, 1681c, 1681e.

The California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq., goes further. It establishes that consumers have the right to know what personal information is collected about them, by whom, and for what purpose. Cal. Civ. Code § 1798.100(a). It gives consumers the right to delete their personal information. Cal. Civ. Code § 1798.105. It prohibits businesses from using personal information for purposes beyond those disclosed to the consumer. Cal. Civ. Code § 1798.100(b). Critically, these rights exist independent of any contract between the businesses holding that data.

The Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809, imposes obligations directly relevant here. Credit monitoring companies qualify as financial institutions under 16 C.F.R. § 313.3(k) and must protect consumers' nonpublic personal information. The GLBA's Safeguards Rule requires covered entities to maintain robust security programs for consumer financial data. 16 C.F.R. Part 314. Nothing in any of these statutory frameworks contemplates consumer financial data being held as a bargaining chip in a commercial dispute between two competing businesses.

Whatever contractual language exists between MFSN and ConsumerDirect regarding data "ownership," that contract cannot override consumers' statutory rights. Private contracts cannot waive or extinguish rights created by federal statute. See Mitsubishi Motors Corp. v. Soler Chrysler-Plymouth, Inc., 473 U.S. 614, 628 (1985). The consumers whose data sits at the center of this dispute did not sign the White Label Agreement. They are not parties to it. They

consented to credit monitoring services — not to having their most sensitive financial information weaponized as leverage in a commercial dispute between two companies competing for their subscription revenue.

B. THE ROLE OF CREDIT REPAIR PARTNERS AND HOW THIS TRANSITION DISRUPTED CONSUMERS AND THE INDUSTRY

To understand the full scope of consumer harm in this case, this Court must understand how the overwhelming majority of MFSN's subscriber base was actually built. This is a critical fact that neither party's filings adequately explain, but which fundamentally shapes the consumer harm analysis.

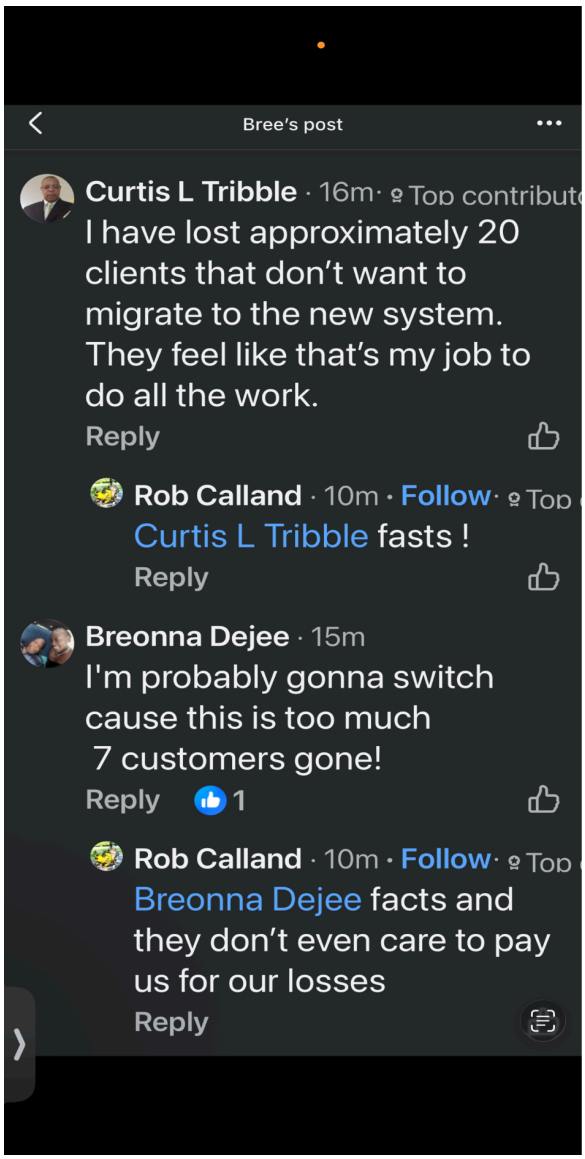
MFSN does not primarily acquire subscribers through direct consumer marketing. The vast majority of MFSN's subscribers are credit repair clients — financially vulnerable individuals who are actively working with credit repair companies to restore their credit profiles. These consumers enroll in MFSN's credit monitoring service at the recommendation of, and in many cases with the direct assistance of, their credit repair company. The credit repair company needs to see monthly credit report updates to track the results of their dispute work and document consumer progress. The consumer signs up for the monitoring service as a functional necessity of the credit repair engagement, not as an independent purchasing decision.

This is not incidental to the business model — it is the business model. MFSN's own filings acknowledge that approximately 80 percent of its customers come through affiliate referrals, and that it maintains commission contracts with approximately 10,000 affiliates. The majority of those affiliates are credit repair companies, credit consultants, and financial professionals who enroll their clients in MFSN as part of an active credit repair engagement. See MFSN TRO Application, Decl. ¶¶ 6, 19.

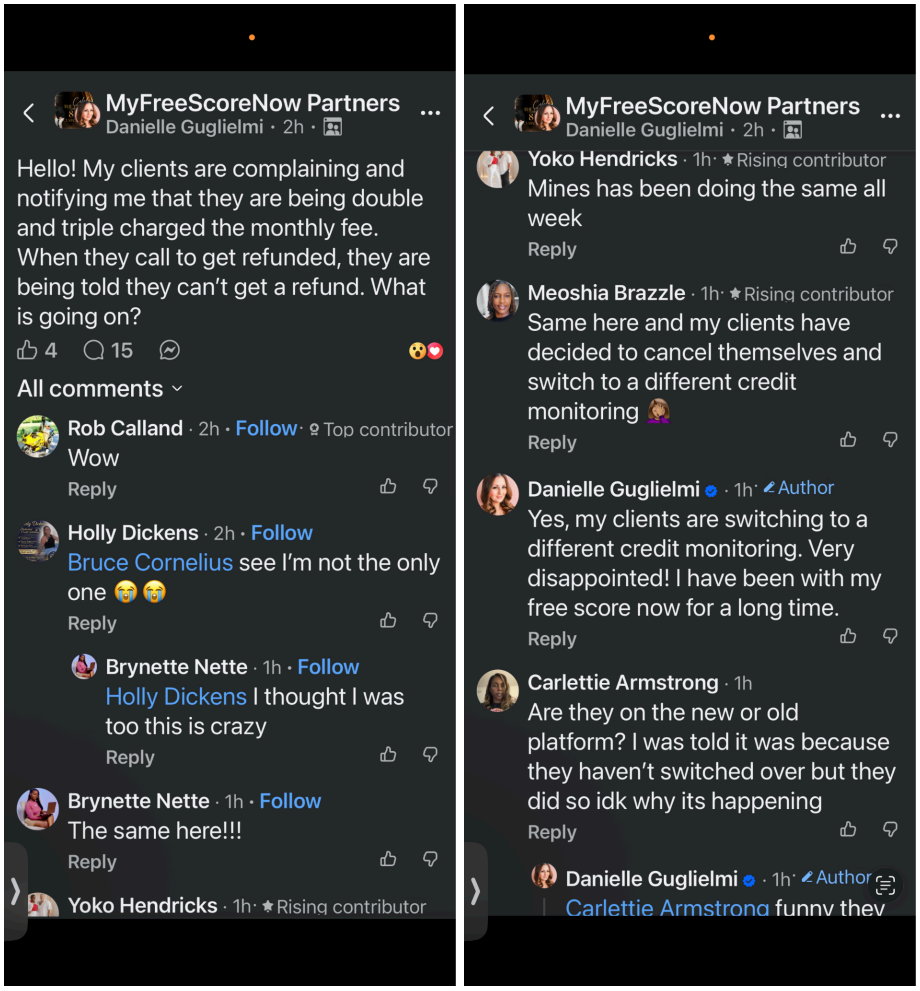
This structural reality carries enormous consequences for the consumer harm analysis. When MFSN's platform became unstable — when consumers were forced through repeated password resets, when promised tools disappeared without disclosure, when billing irregularities occurred — the harm did not fall on sophisticated individual consumers who had independently chosen a credit monitoring subscription. The harm fell on people already in the middle of a credit repair process, who were enrolled in the service by a trusted credit repair professional, who had no independent relationship with MFSN, and who had no practical understanding of why their monitoring access was suddenly disrupted.

From the perspective of the credit repair professional, this created an untenable situation. A credit repair company's entire value proposition to its client rests on its ability to track, document, and demonstrate credit score and report changes month over month. When the monitoring platform becomes unreliable, the credit repair company cannot do its job. Clients who cannot see their credit reports, who are being asked to reset their passwords, who receive conflicting information about their enrollment status, lose faith in their credit repair company — not in MFSN, whose name they may barely recognize. The credit repair company bears the reputational damage for a platform failure entirely outside its control.

This harm is not speculative. Documented public statements from members of MFSN's own official partner Facebook group — "MyFreeScoreNow Partners" — establish that multiple credit repair professionals lost clients directly as a result of MFSN's platform transition failures. Curtis L. Tribble, a top contributor in the partner group, publicly stated: "I have lost approximately 20 clients that don't want to migrate to the new system. They feel like that's my job to do all the work."



Breonna Dejee reported losing 7 clients. Rob Calland, another member, stated that MFSN would not compensate partners for their losses. Meoshia Brazzle reported that her clients decided to cancel and switch to a different credit monitoring service entirely. Danielle Guglielmi, a verified partner, stated that her clients were switching to different monitoring services and expressed that she had been with MFSN for a long time and was "very disappointed." These are not anonymous complaints. They are identified credit repair professionals, posting in MFSN's own official partner community, describing documented client losses attributable to MFSN's transition mismanagement.



The harm cascades in a way that this Court should understand clearly. A consumer who loses confidence in their monitoring access does not simply pause their credit repair — they abandon it. They fire their credit repair company, whom they blame for the disruption. They end up in the same or worse financial position they started in, often after months of payments. This is not a commercial harm between sophisticated business entities. This is a consumer protection failure with real human consequences for the most financially vulnerable segment of the credit monitoring market.

C. MFSN'S PLATFORM MIGRATION WAS DECEPTIVE, GENERATED SYSTEMATIC DOUBLE AND TRIPLE BILLING, AND MFSN REFUSED REFUNDS

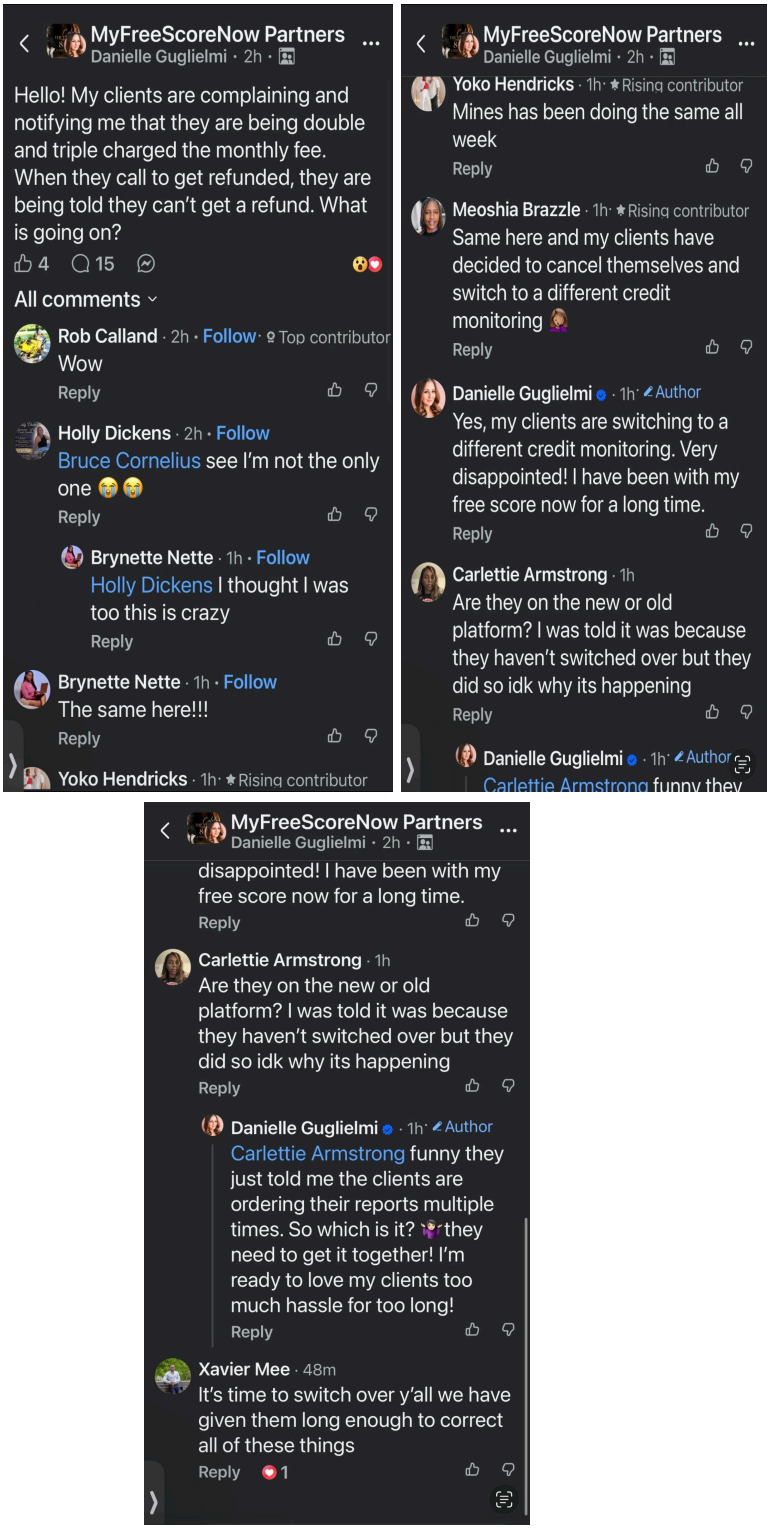
The manner in which MFSN marketed its platform transition to consumers raises serious questions under both federal and California consumer protection law. MFSN characterized its migration away from ConsumerDirect's SmartCredit platform as an "upgrade" — a term that uniformly implies improvement and enhanced functionality. This characterization was materially misleading, and the documented billing consequences of that migration constitute potential violations of federal consumer financial protection statutes.

ConsumerDirect's SmartCredit platform, which consumers had been using through MFSN's white label product, offered a robust suite of credit management tools developed over more than two decades and protected by 23 issued patents. These tools included sophisticated credit monitoring capabilities, privacy tools, money management tools, analytics, and consumer-facing features that MFSN's new platform did not replicate at launch. ConsumerDirect's own cancellation email to transitioning consumers — sent to consumers whose accounts were being closed — stated explicitly and in bold that "any new membership is NOT provided through ConsumerDirect and will be a different product with different features and terms," and advised consumers that they were "responsible for reviewing the provider name, features, and billing terms" before enrolling in any new service. ConsumerDirect told consumers the truth. MFSN told consumers they were getting an upgrade.

The FTC Act's prohibition on unfair or deceptive acts or practices, 15 U.S.C. § 45(a), reaches exactly this type of conduct. Characterizing a platform migration as an "upgrade" when the migrating consumer will lose access to features and tools they currently have is a classic deceptive omission — a half-truth that creates a false impression. FTC v. Sterling Drug, Inc., 317 F.2d 669, 674 (2d Cir. 1963). California's CLRA specifically prohibits misrepresenting the quality of goods or services. Cal. Civ. Code § 1770(a)(5), (7). Moreover, MFSN's own partner community confirms that the platform's reporting functionality was unreliable at launch. A credit repair partner posted in the MyFreeScoreNow Partners group that "on the dashboard like on the client side when y'all log into your account, it will show you have no negative accounts" — showing everything green — while "when we pull it into the CRM on our side, the negative accounts do pop up" showing 90 and 120-day derogatory accounts.

A platform that actively conceals derogatory credit information from consumers while showing it to partner-side CRM users is not an upgrade. It is a material data accuracy failure with potential FCRA implications.

The billing failures associated with this transition are the most immediately actionable consumer harm in this record. Danielle Guglielmi, a verified MFSN partner, posted publicly in the MyFreeScoreNow Partners group that her clients were "being double and triple charged the monthly fee" and that when consumers called to request refunds, they were told "they can't get a refund." Multiple partners — including Holly Dickens, Brynette Nette, and Yoko Hendricks — publicly confirmed experiencing the same billing failures with their clients.



Cameron Webster reported that his client signed up for the upgrade expecting the old account to be closed, resulting in being "billed twice for the same platform." Anne Black reported charges on March 12 and again on March 15, three days apart, on her husband's account after he completed the migration. When Danielle Guglielmi sought an explanation from MFSN

for why consumers on the new platform were being charged multiple times, she was told that the consumers were "ordering their reports multiple times" — placing the blame on the consumers themselves for a systemic billing error.

The refusal to issue refunds for duplicate and triplicate charges is not a billing dispute. It is a potential violation of the Electronic Fund Transfer Act's error resolution provisions, 15 U.S.C. § 1693f, which requires financial institutions to investigate and correct billing errors and prohibits them from refusing to refund unauthorized charges. It also implicates Regulation E's requirements for error resolution procedures. 12 C.F.R. § 1005.11. Blaming consumers for charges generated by a platform migration they did not control, and then refusing refunds on that basis, is the kind of conduct that draws CFPB enforcement attention. The CFPB has supervisory authority over larger participants in consumer financial data markets and has increasingly focused on billing practices in subscription-based financial services.

California's Consumers Legal Remedies Act, Cal. Civ. Code § 1770, provides independent state law bases for the same conclusion. The CLRA specifically prohibits representing that goods or services have characteristics they do not have, misrepresenting the quality of services, and advertising services with intent not to supply them as advertised. Cal. Civ. Code § 1770(a)(5), (7), (9). A consumer who was promised an upgrade, lost access to features she previously had, was charged two or three times for services she could not fully access, and was told she could not get a refund has actionable claims under both the CLRA and the UCL.

D. REPEATED PASSWORD RESETS DURING ACTIVE TERMINATION PROCEEDINGS CAUSED QUANTIFIED CLIENT LOSS AND RAISE SERIOUS DATA SECURITY QUESTIONS

Among the most concrete and verifiable harms documented in connection with this transition is the fact that MFSN consumers were required to reset their account passwords on at least three separate occasions during the period in which MFSN and ConsumerDirect were negotiating and then executing the termination of their White Label Agreement. This is not a minor inconvenience. In the context of a credit monitoring service used primarily by credit repair clients, it is a material harm with documented consequences.

Holly Dickens, an MFSN partner, stated publicly in the MyFreeScoreNow Partners group: "I was only able to get maybe 1/2 of my clients to even do the password reset so idk how I'm gonna get them all to perform the upgrade." Tyler Dickens confirmed in the same thread: "we're losing clients and referrals bc of this." Korea Brinkley, the original poster in that thread, summarized the situation plainly: "it's affecting how I operate my business" and noted that the new software "definitely looks mediocre." Xavier Mee responded: "It's time to switch over y'all we have given them long enough to correct all of these things." These are partners telling each other, in MFSN's own community forum, that they are losing clients and considering leaving the platform entirely — not because of the litigation, but because of the operational failures MFSN created during the transition.

Credit monitoring consumers are, by definition, people who have experienced financial difficulty. Many have also experienced identity theft or credit fraud — conditions that frequently

precipitate the need for credit repair. These consumers have been trained, correctly, to treat unexpected requests to reset account credentials as a potential security breach indicator. When MFSN required consumers to reset their passwords repeatedly during a period of obvious platform instability — while their personal financial data was simultaneously the subject of a corporate dispute between MFSN and ConsumerDirect — many consumers made the rational decision to disengage entirely. The credit repair company bore the reputational consequences of that decision.

There is also a data integrity dimension that this Court should not overlook. Beyond the password reset issue, Yoko Hendricks reported in the MyFreeScoreNow Partners group that a significant number of her clients' Equifax scores had completely disappeared from the platform — not due to any address error, which she had verified directly with Equifax. A credit monitoring platform that fails to display a consumer's credit score from one of the three major bureaus is not functioning as represented. Under the FCRA, credit monitoring companies have obligations around the completeness and accuracy of the information they provide to consumers. 15 U.S.C. § 1681e. A platform that hides derogatory accounts on the consumer-facing dashboard while displaying them in the partner CRM, and that causes Equifax scores to disappear entirely for some users, raises serious questions about whether MFSN's new platform met the accuracy and completeness standards required by federal law at the time it was deployed.

The GLBA Safeguards Rule requires covered financial institutions to maintain a written information security program that protects customer information. 16 C.F.R. § 314.4. Repeated credential resets during a disputed data transfer involving Social Security numbers and full credit card information are not consistent with a mature, stable security program. This is a compliance question that the FTC, which enforces the Safeguards Rule, would have standing to investigate independent of anything this Court decides.

E. REMAND TO CALIFORNIA STATE COURT WOULD BETTER PROTECT THE CONSUMER INTERESTS AT THE HEART OF THIS DISPUTE

Amicus respectfully urges this Court to consider remanding the removed action — originally filed by ConsumerDirect in Orange County Superior Court — back to California state court, and to consolidate resolution of the consumer protection dimensions of this dispute in that forum. This Court has discretion to consider this question in connection with any remand motion that may be pending or forthcoming, and amicus raises it here as a matter of public interest rather than advocacy for either corporate party.

California state courts have historically provided stronger and more comprehensive protections for consumers in data-related disputes than the federal framework alone supplies. This is not a close question. The California Consumer Privacy Act, operative since January 2020 and significantly strengthened by the California Privacy Rights Act effective January 2023, creates a private right of action for consumers whose personal information is subject to unauthorized access, exfiltration, or disclosure resulting from a business's failure to implement reasonable security measures. Cal. Civ. Code § 1798.150. This private right of action does not exist under federal law — the FCRA and GLBA do not create equivalent individual consumer enforcement rights for data handling failures short of a formal data breach.

The California Consumers Legal Remedies Act, Cal. Civ. Code § 1770 et seq., provides consumers with the right to bring class actions for deceptive business practices and awards injunctive relief, restitution, and attorney's fees. The CLRA's protections apply squarely to the conduct described in this brief — the misrepresentation of a platform "upgrade" that stripped consumers of features without disclosure, the double billing during transition, and the repeated credential disruptions. A California state court applying the CLRA can provide remedies to the consumer class that a federal court sitting in diversity jurisdiction, applying contract law between sophisticated commercial parties, may not be equipped to address.

The Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 et seq., allows any person acting in the public interest to bring suit to enjoin unfair business practices. This is broader than any federal analog. It does not require individualized proof of consumer harm and can reach conduct that is merely "unfair" even if not technically unlawful. The conduct described in this brief — inducing consumers to migrate to an inferior platform through deceptive "upgrade" marketing, billing them during a period of disrupted access, and subjecting them to repeated security-related credential changes — fits squarely within the UCL's reach.

Amicus is mindful that the removal to federal court was executed by MFSN and Cornelius as defendants in ConsumerDirect's state court action, and that ConsumerDirect may separately seek remand. The consumer protection argument for remand is distinct from and independent of the contractual forum selection argument that ConsumerDirect will likely raise. The point is not that one forum is procedurally preferable for the contract dispute — it is that California state court offers consumers affected by this litigation a more complete set of rights and remedies than federal court does, and that this distinction matters to the 115,000 people whose data is at stake.

Alternatively, if this Court retains jurisdiction, amicus respectfully urges that any equitable relief ordered include provisions specifically protecting consumer interests: an order that no consumer be billed for services they cannot access during the transition period; an order that the data transfer be conducted under appropriate security protocols with independent verification; and an order that consumers be notified accurately — without the deceptive "upgrade" framing — of any changes to the services and features available to them on any new platform.

F. IN THE ALTERNATIVE, THIS COURT SHOULD APPOINT A SPECIAL MASTER TO ADMINISTER CONSUMER DATA PENDING RESOLUTION, WITH COSTS BORNE BY MFSN IF IT IS FOUND LIABLE

If this Court declines to remand the removed action to California state court, amicus respectfully urges the Court to consider an alternative remedy that neither party has proposed but that would serve both the immediate interests of justice and the long-term interests of the consumers whose data sits at the center of this dispute: the appointment of a neutral special master pursuant to Federal Rule of Civil Procedure 53 to take temporary administrative custody of the consumer data at issue and oversee its handling pending final resolution.

Federal Rule of Civil Procedure 53(a)(1)(B) authorizes a district court to appoint a special master to "address pretrial and posttrial matters that cannot be effectively and timely addressed by an available district judge or magistrate judge." The consumer data dispute in this case is precisely such a matter. This Court is being asked to rule on urgent data custody questions involving the sensitive personal and financial information of over 115,000 consumers — their Social Security numbers, credit card information, billing histories, and credit report access credentials — while simultaneously managing complex trade secret litigation, a removed state court action, competing TRO applications, and potential remand proceedings. A neutral special master with expertise in data privacy, financial services, or consumer protection could administer the consumer data custodianship question with the focused attention it demands, without consuming the Court's docket capacity on a matter that is, at its core, a data management and consumer protection problem rather than a legal one.

The special master's mandate should be specifically structured to protect consumer interests rather than to adjudicate the parties' commercial dispute. Amicus proposes that the special master's role include: (1) taking temporary neutral custody of the consumer data currently held by ConsumerDirect, ensuring it remains securely maintained on ConsumerDirect's platform — which has an established security record — pending resolution; (2) conducting or commissioning an independent security assessment of MFSN's new platform before authorizing any data transfer, with input from qualified cybersecurity professionals rather than relying solely on MFSN's chosen vendor; (3) receiving input from industry stakeholders, consumer advocacy organizations, and relevant nonprofit consumer protection entities regarding what data transfer and transition protocols would best serve consumer interests; (4) overseeing any eventual data migration to ensure it is conducted securely, completely, and without billing disruption to consumers; and (5) reporting to the Court on any consumer billing irregularities identified during the pendency of the special master's oversight.

The stakeholder input component of this proposal deserves specific attention. The credit monitoring and credit repair industries are interconnected ecosystems with established professional communities, trade associations, and advocacy organizations that have deep expertise in exactly the consumer harm questions this case presents. The National Foundation for Credit Counseling, consumer law clinics, state consumer protection offices, and organizations like the Consumer Federation of America have institutional knowledge about how platform transitions in financial services affect vulnerable consumers that neither party's litigation counsel possesses. A special master who consults these voices before recommending a data transfer protocol would produce a result that actually serves consumers — not just the party that wins the contract argument.

On the question of costs: Federal Rule of Civil Procedure 53(g) provides that the Court must allocate the special master's compensation among the parties or tax it as costs. Amicus respectfully submits that if this Court appoints a special master and subsequently finds that MFSN materially breached the White Label Agreement, engaged in deceptive migration marketing, or caused the consumer billing harms documented in this brief, the full cost of the special master's appointment should be taxed against MFSN. The consumers who are the beneficiaries of this relief should bear none of it. ConsumerDirect, which has complied with its contractual data security obligations and whose platform has maintained a record of consumer data security, should not be required to absorb costs attributable to MFSN's failure to execute an

orderly transition. The party whose conduct necessitated court intervention should bear the cost of that intervention.

This proposal offers the Court a practical path that neither party's filings contemplate. Rather than choosing between granting MFSN's TRO and immediately transferring 115,000 consumers' most sensitive financial data to a platform whose security remains disputed, or denying the TRO and leaving that data in the hands of a party that has demonstrably used it for competitive solicitation, the Court could place the data under neutral professional oversight while the litigation proceeds on a normal schedule. The consumers whose information is at stake deserve nothing less.

G. CONSUMERS HOLD COMMON LAW AND CONSTITUTIONAL RIGHTS IN THEIR PERSONAL FINANCIAL DATA THAT EXIST INDEPENDENT OF STATUTE AND INDEPENDENT OF ANY CONTRACT BETWEEN THESE PARTIES

Amicus recognizes that it is not the province of federal courts to make law, and this brief does not ask this Court to do so. What amicus does urge is that this Court recognize, in the equitable analysis it undertakes, that the question of consumer data rights in this case is not exhausted by the statutory framework discussed above. Consumers hold common law privacy rights in their personal financial information — rights that predate the FCRA, the GLBA, and the CCPA — and those rights are protected by the Ninth Amendment to the United States Constitution.

The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people." U.S. Const. amend. IX. The Supreme Court has recognized that the Constitution protects unenumerated rights retained by the people, including rights of privacy and personal autonomy that are not specifically named in the Bill of Rights. Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (recognizing "zones of privacy" created by the penumbras of the Bill of Rights); see also Whalen v. Roe, 429 U.S. 589, 599 (1977) (recognizing constitutional protection for "the individual interest in avoiding disclosure of personal matters").

The right of an individual to control the dissemination and use of their own personal financial information — their Social Security number, their credit card account details, their billing history, their credit report — is precisely the kind of fundamental personal interest that the Ninth Amendment was designed to protect. This is not a novel or radical proposition. The Supreme Court in Whalen v. Roe specifically identified the "interest in avoiding disclosure of personal matters" as a constitutionally protected privacy interest. 429 U.S. at 599. The Court of Appeals for the Ninth Circuit has recognized that individuals have a constitutionally protected privacy interest in their financial information. See, e.g., In re Crawford, 194 F.3d 954, 958 (9th Cir. 1999) (recognizing privacy interest in Social Security numbers); Planned Parenthood of S. Ariz. v. Lawall, 307 F.3d 783, 789 (9th Cir. 2002) (privacy rights include control over personal information).

The constitutional dimension of this case matters in a specific and practical way. Both parties before this Court have framed the consumer data question as a contractual one — who owns the data under the White Label Agreement. Amicus submits that this framing is

fundamentally incomplete. Consumer financial data is not merely a contractual asset. It is the most intimate financial expression of a person's economic life. A consumer's Social Security number, credit card number, and credit history are not widgets to be transferred between companies in a commercial dispute. They are personal identifiers that, if misused, can destroy a person's financial life for years. The consumers who enrolled in MFSN's service — many of them already recovering from exactly that kind of financial harm — did not surrender their constitutional privacy interests when they signed up for credit monitoring. They did not consent to becoming the subject of a corporate custody battle between two competing businesses.

Amicus is not asking this Court to create a new constitutional right or to make law. The right exists. What amicus asks is that this Court's equitable analysis — in fashioning any TRO, preliminary injunction, or other relief — be informed by the recognition that the consumers whose data is at issue have interests that transcend the contract between MFSN and ConsumerDirect, interests that cannot be waived by either party on the consumers' behalf, and interests that the Constitution itself recognizes as deserving protection.

The credit monitoring industry is a rapidly growing field that touches the financial lives of tens of millions of Americans. The CFPB has identified data broker and data aggregator practices as a priority supervisory area. Congress has held hearings on consumer data rights. State legislatures across the country are passing comprehensive privacy legislation modeled on California's framework. This case — involving over 115,000 consumers' most sensitive financial data, a chaotic platform transition, documented billing abuses, and a complete absence of any party advocating for the consumers themselves — is precisely the kind of case that can serve as a vehicle for this Court to articulate clearly that consumer financial data is held in trust, that the people to whom it belongs retain constitutional and common law rights in it that no private contract can extinguish, and that courts of equity will protect those rights when the parties before them will not.

Amicus does not ask this Court to resolve the constitutional question definitively. Amicus asks this Court to acknowledge it — to note, in whatever relief it orders, that consumer data rights are not simply a function of who wins the contract dispute, and that the 115,000 people whose information is at stake are not bystanders in their own financial lives. They are rights-holders. And they deserve a court that remembers that.

V. CONCLUSION

The consumers at the center of this dispute are not abstractions. They are people who are already financially vulnerable, who enrolled in a credit monitoring service because their credit repair company told them they needed to, who do not understand the corporate relationship between MFSN and ConsumerDirect, and who have been subjected to platform instability, deceptive marketing, documented double and triple billing with refunds refused, and repeated security disruptions that caused real harm to their credit repair progress and their relationships with the professionals helping them.

For the foregoing reasons, amicus curiae Joeziel Vazquez-Davila respectfully urges this Court to: (1) make clear in any relief ordered that consumer credit data is held in trust for consumers and cannot be used as corporate leverage regardless of what any contract between

businesses provides; (2) consider remanding the removed action to California state court where consumer protection law is more comprehensive and where a private right of action exists for the data handling failures described herein; (3) in the alternative, appoint a neutral special master under Federal Rule of Civil Procedure 53 to administer consumer data custody with input from industry stakeholders and consumer advocacy organizations, with costs taxed to MFSN if it is found liable; (4) order immediate suspension of consumer billing during any data transition period and require independent security verification before any data transfer is authorized; (5) acknowledge that consumers hold constitutional and common law privacy rights in their personal financial data that transcend the contractual dispute between the parties and that cannot be waived by either party on consumers' behalf; and (6) ensure that any resolution of this dispute is structured to restore, not further disrupt, the ability of the credit repair professionals who depend on stable credit monitoring infrastructure to serve their clients.

The consumers whose data is at issue in this case did not choose to be caught in the middle of this dispute. They are rights-holders. They deserve a court that sees them.

Respectfully submitted,

Joeziel Joey Vazquez

Joeziel Vazquez-Davila, Pro Se
CEO & Founder, Credlocity Business Group LLC
1500 Chestnut Street, Suite 2
Philadelphia, PA 19102
admin@credlocity.com

Board Certified Credit Consultant (BCCC)
Certified Credit Score Consultant (CCSC)
Certified Credit Repair Specialist (CCRS)

Dated: 4/28/2026

CERTIFICATE OF SERVICE

I hereby certify that on this date, I caused a true and correct copy of the foregoing Brief of Amicus Curiae to be served upon counsel for all parties in this action via the Court's Electronic Case Filing system and/or by first-class U.S. mail to the addresses listed on the docket.

Dated: 4/28/2026

Joeziel Vazquez-Davila, Pro Se