

STATE OF VERMONT

SUPERIOR COURT
CHITTENDEN UNIT

CIVIL DIVISION
DOCKET NO. _____

STATE OF VERMONT,)
)
 Plaintiff,)
)
v.)
)
CLEARVIEW AI, INC.,)
)
 Defendant.)

VERMONT SUPERIOR COURT
FILED

MAR 10 2020

Chittenden Unit

STATE OF VERMONT'S MOTION FOR PRELIMINARY INJUNCTION

STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

Justin Kolber
Ryan Kriger
Jill Abrams
Assistant Attorneys General
Office of the Attorney General
109 State Street
Montpelier, VT 05609-1001
(802) 828-3171
justin.kolber@vermont.gov
ryan.kriger@vermont.gov
jill.abrams@vermont.gov

Filed March 10, 2020

Table of Contents

Table of Authorities	ii
Preliminary Statement	2
Background and Facts	5
Clearview Collects and Stores 3,000,000,000 Photos.....	6
Clearview Collects and Stores Photos of Minors.....	8
Clearview Uses Facial Recognition AI to Match People	9
Clearview Sells its Technology to Whomever Clearview Decides	10
Clearview Misrepresents its Product.....	11
Argument	14
I. Applicable Standards for an Injunction	14
A. An Injunction is Authorized by Statute	14
B. Legal Standards for a Statutory Injunction.....	15
II. Overview of Vermont Consumer Protection Act	17
A. Unfairness	18
B. Deception	19
III. Defendant Clearview Has Committed Unfair and Deceptive Acts	20
A. Defendant's conduct is unfair because it violates consumers' right and expectation of privacy.....	20
1. <i>Right to privacy generally</i>	21
2. <i>The right to privacy develops with technology</i>	22
3. <i>The right to privacy is an actionable right</i>	26
4. <i>Clearview has engaged in unfair trade practices by violating Vermonters'</i> <i>right to privacy</i>	27
B. Defendant's conduct is unfair because it violates contracts and website terms of service..	38
C. Defendant's conduct is unfair because it fails to protect consumers' data.	41
D. Defendant's conduct is deceptive because of several misrepresentations around its privacy protections, data security, and product.	42
E. Defendant's conduct is unfair because it is immoral, unethical and oppressive.....	45
F. Defendant's conduct violates Vermont's Fraudulent Acquisition of Data Law.	50
Request for Relief	51
Conclusion	54

Table of Authorities

Cases

<i>Bernhardt v. Polygraphic Co.</i> , 350 U.S. 198 (1956).....	26
<i>Birnbaum v. United States</i> , 588 F.2d 319 (2d Cir. 1978)	21, 26
<i>Cappello v. Walmart Inc.</i> , 394 F. Supp. 3d 1015 (N.D. Cal. 2019).....	39
<i>Carpenter v. United States</i> 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018)	<i>passim</i>
<i>Carter v. Gugliuzzi</i> , 168 Vt. 48, A.2d 17 (1998)	17, 19, 44
<i>Centerline Equip. Corp. v. Banner Pers. Serv., Inc.</i> , 545 F. Supp. 2d 768 (N.D. Ill. 2008).....	47
<i>Chick Kam Choo v. Exxon Corp.</i> , 486 U.S. 140 (1988)	15
<i>Christie v. Dalmig, Inc.</i> , 136 Vt. 597, 396 A.2d 1385 (1979)	<i>passim</i>
<i>Cooper v. Slice Techs., Inc.</i> , No. 17-CV-7102 (JPO), 2018 WL 2727888 (S.D.N.Y. June 6, 2018).....	29
<i>Cox Broadcasting Corp. v. Cohn</i> , 420 U.S. 469 (1975)	21
<i>Cox v. Sears Roebuck & Co.</i> , 138 N.J. 2, 647 A.2d 454 (1994)	45
<i>Denton v. Chittenden Bank</i> , 163 Vt. 62, 655 A.2d 703 (1994).....	21
<i>Dernier v. Mortgage Network, Inc.</i> , 195 Vt. 113 A.3d 465, 2013 VT 96	18
<i>Douglas v. U.S. Dist. Court for Cent. Dist. of California</i> , 495 F.3d 1062 (9th Cir. 2007)	40
<i>Edenfield v. Fane</i> , 507 U.S. 761 (1993)	22
<i>EF Cultural Travel BV v. Explorica, Inc.</i> , 274 F.3d 577 (1st Cir. 2001).....	39
<i>Envtl. Def. Fund v. Lamphier</i> , 714 F.2d 331 (4th Cir. 1983)	16
<i>Folgelstrom v. Lamps Plus, Inc.</i> , 195 Cal. App. 4th 986 (Ca. 2011).....	28
<i>FTC v. Accusearch Inc.</i> , 570 F.3d 1187 (10th Cir. 2009)	40
<i>FTC v. Equifax Inc.</i> , Case No. 1:19-mi-99999 (N.D. Ga. July 22, 2019).....	41
<i>FTC v. InMobi Pte Ltd</i> , No. 3:16-cv-3474 (N.D. Cal. June 22, 2016).....	33
<i>FTC v. National Lead</i> , 352 U.S. 419 (1959)	51
<i>FTC v. Sperry & Hutchinson Co.</i> , 405 U.S. 233 (1972)	18, 19
<i>FTC v. Wyndham Worldwide Corp.</i> , 799 F.3d 236 (3d Cir. 2015).....	41
<i>Gantchev v. Predicto Mobile</i> , No. 09 C 2312, LLC, 2009 WL 3055317 (N.D. Ill. Sept. 18, 2009).....	47
<i>Gill v. Hearst Pub. Co.</i> , 40 Cal. 2d 224, 253 P.2d 441 (1953)	34

<i>Goldman v. Breitbart News Network, LLC</i> , 302 F. Supp. 3d 585 (S.D.N.Y. 2018)	40, 49
<i>Gonzales v. Uber Techs., Inc.</i> , 305 F. Supp. 3d 1078 (N.D. Cal. 2018).....	30
<i>Harris v. Carbonneau</i> , 165 Vt. 433, 685 A.2d 296 (1996).....	27
<i>Henderson v. Byrd</i> , 133 F.2d 515 (2d Cir. 1943).....	16
<i>Henderson v. United Student Aid Funds, Inc.</i> , 918 F.3d 1068 (9th Cir. 2019).....	48
<i>Hodgdon v. Mount Mansfield Co.</i> , 160 Vt. 150, 624 A.2d 1122 (1992)	27
<i>In re Anthem, Inc. Data Breach Litig.</i> , 162 F. Supp. 3d 953 (N.D. Cal. 2016)	41
<i>In re Cliffdale Assocs., Inc.</i> , No. 9156, 1984 WL 565319 (FTC Mar. 23, 1984).....	19
<i>In re Google Inc. Cookie Placement Consumer Privacy Litig.</i> , 806 F.3d 125 (3d Cir. 2015)	5, 30, 32
<i>In re Google Location History Litig.</i> , No. 5:18-CV-05062-EJD, 2019 WL 6911951 (N.D. Cal. Dec. 19, 2019)	31
<i>In re J.G.</i> , 160 Vt. 250 (1993)	16
<i>In re: Cambridge Analytica, LLC</i> , Docket No. 9383 (FTC Nov. 25, 2019).....	44
<i>In re: Epic Media Group, LLC</i> , Docket No. C-4389 (FTC Mar. 19, 2013).....	42
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001).....	37
<i>McDonald v. Killoo ApS</i> , 385 F. Supp. 3d 1022 (N.D. Cal. 2019)	32
<i>McIntyre v. Ohio Elections Comm’n</i> , 514 U.S. 334 (1995).....	22
<i>Minnesota ex rel. Hatch v. Sunbelt Commc'ns & Mktg.</i> , 282 F. Supp. 2d 976 (D. Minn. 2002)	15, 22
<i>Mount v. PulsePoint, Inc.</i> , 684 F. App’x 32 (2d Cir. 2017).....	31
<i>Orkin Exterminating Co., Inc. v. FTC</i> , 849 F.2d 1354 (11 th Cir. 1988).....	18
<i>Patel v. Facebook, Inc.</i> , 932 F.3d 1264 (9th Cir. 2019)	30, 32, 52
<i>People ex rel. Hartigan v. Stianos</i> , 475 N.E.2d 1024 (Ill. App. Ct. 1985).....	17
<i>Rathe Salvage, Inc. v. R. Brown & Sons, Inc.</i> , 184 Vt. 355, 965 A.2d 460, 2008 VT 99 (2008) ...	40
<i>State of Vermont v. CSA-Credit Solutions of Am., LLC & Doug Van Arsdale</i> , Dec. and Order: Mot. for Summ. J. (Vt. Super. Ct. March 5, 2012).....	19
<i>State v. Fonk’s Mobile Home Park & Sales</i> , 343 N.W.2d 820 (Wis. Ct. App. 1983) ..	17
<i>State v. Koenig</i> , 2016 VT 65, 202 Vt. 243, 148 A.3d 977 (2016)	38
<i>State v. VanBuren</i> , 2018 VT 95, 214 A.3d 791 (Vt. 2019).....	22, 23
<i>TravelJungle v. Am. Airlines, Inc.</i> , 212 S.W.3d 841 (Tex. App. 2006).....	6

<i>U.S. Dep’t of Justice v. Reporters Comm. for Freedom of the Press</i> , 489 U.S. 749 (1989).....	21
<i>United States v. City and County of San Francisco</i> , 310 U.S. 16 (1940)	16
<i>United States v. Estate Pres. Servs.</i> , 202 F.3d 1093 (9th Cir. 2000)	16
<i>United States v. Jones</i> , 565 U.S. 400 (2012).	23, 35, 37
<i>United States v. Rodriguez</i> , 628 F.3d 1258 (11th Cir. 2010)	39
<i>United States v. Weingold</i> , 844 F. Supp. 1560 (D. N.J. 1994)	16
<i>United States v. White</i> , 769 F.2d 511 (8th Cir. 1985)	16
<i>Votto v. Am. Car Rental, Inc.</i> , 273 Conn. 478, 871 A.2d 981 (2005).....	48
<i>Webster v. Milbourn</i> , 759 S.W.2d 862 (Mo. Ct. App. 1988)	17
<i>Weinstein v. Leonard</i> , 2015 VT 136, 200 Vt. 615, 134 A.3d 547 (2015)	27, 28
<i>Williams v. Superior Court</i> , 3 Cal. 5th 531, 398 P.3d 69 (2017)	30

Statutes

9 V.S.A. § 2431	1, 50, 52
9 V.S.A. § 2451	1
9 V.S.A. § 2453	17, 18
9 V.S.A. § 2458	1, 14

Other Authorities

Eli A. Meltz, <i>No Harm, No Foul? “Attempted” Invasion of Privacy and the Tort of Intrusion Upon Seclusion</i> , 83 Fordham L. Rev. 3431 (2015)	24
FTC, <i>Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies</i> (Oct. 2012)	<i>passim</i>
Georgetown Law Center on Privacy & Technology, <i>The Perpetual Line-Up: Unregulated Police Face Recognition in America</i> (Oct. 18, 2016).....	<i>passim</i>
Giorgio Bovenzi, <i>Liabilities of System Operators on the Internet</i> , 11 Berkeley Tech. L.J. 93 (1996)	22
Justin H. Dion & Nicholas M. Smith, <i>Consumer Protection: Exploring Private Causes of Action for Victims of Data Breaches</i> , 41 W. New Eng. L. Rev. 253 (2019)	44
Restatement (Second) of Torts § 652 (1977)	26, 27
Robert D. Lang & Lenore E. Benessere, <i>Alexa, Siri, Bixby, Google’s Assistant, and Cortana Testifying in Court</i> , 74 J. Mo. B. 20, (2018).....	26

Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890)... 23

Sean O'Reilly, *Nominative Fair Use and Internet Aggregators: Copyright and Trademark Challenges Posed by Bots, Web Crawlers and Screen-Scraping Technologies*, 19 Loy. Consumer L. Rev. 273 (2007) 6

Rules

Vermont Rule of Civil Procedure 65(b)(1) 1

Treatises

11A Wright, Miller & Kane, *Federal Practice and Procedure: Civil 2d* § 2948 (1995) 16

Dean W. Prosser, *The Law of Torts* (4th ed. 1971) 21

Constitutional Provisions

Article 11 of the Vermont Constitution..... 22

STATE OF VERMONT

SUPERIOR COURT
CHITTENDEN UNIT

CIVIL DIVISION
DOCKET NO. _____

STATE OF VERMONT,)
)
 Plaintiff,)
)
v.)
)
CLEARVIEW AI, INC.,)
)
 Defendant.)

STATE OF VERMONT’S MOTION FOR PRELIMINARY INJUNCTION

NOW COMES The State of Vermont, and pursuant to Vermont Rule of Civil Procedure 65(b)(1) and 9 V.S.A. § 2458(a), moves this Court for preliminary relief to enjoin Clearview AI, Inc. (“Defendant” or “Clearview”) from collecting, storing, and making available images of Vermonters in its surveillance database. Clearview’s unauthorized and illegal collection of photos from Vermonters, including children, for the purpose of building and selling a facial recognition and surveillance system, together with its misrepresentations about the product, constitute unfair and deceptive acts and practices that violate Vermont’s Consumer Protection Act, 9 V.S.A. § 2451 *et seq.* and Vermont’s Fraudulent Acquisition of Data Law, 9 V.S.A. § 2431. This Court should grant this Motion for Preliminary Injunction because Vermonters’ substantial privacy and security interests are at immediate risk, especially in light of the recent data breach at Clearview.

In furtherance of this Motion for Preliminary Injunction, the State of Vermont submits the following Memorandum of Law.

MEMORANDUM OF LAW

After a preliminary statement and description of Clearview's conduct, the first section of this memorandum discusses the applicable standard for granting injunctive relief; the second section outlines the legal principles pertinent to consumer protection violations; and the third section applies those principles to the facts of Defendant's conduct. Combined, the facts and legal standards demonstrate that a preliminary injunction should be issued here.

Preliminary Statement

Clearview AI has embarked on a course of conduct which, if permitted to continue, will have serious and irreversible effects on the people of Vermont. Clearview has brought surveillance technology to market without appropriate safeguards, data security, or consumer consent, which is already producing negative repercussions.

Our fundamental freedoms: to express ourselves, to gather, to go outside and take a walk around town, rely on an underlying right: privacy. Our daily activities often presume a degree of anonymity that we do not appreciate until it is gone, as any celebrity can attest to. The opposite of privacy is surveillance – the state of affairs where we are being watched, tracked, and analyzed constantly.

Technology has, for better or worse, made surveillance cheap, effective, and in some ways ubiquitous. Surveillance is also profitable. As our lives increasingly

shift to an online existence, surveillance in the form of tracking our website browsing, our search history, and our shopping habits, has become a matter of course. We are known to hundreds of businesses, advertisers, and sometimes government agencies, from the moment we log on.

However, we still have the option of turning off the computer, going outside, and enjoying our anonymity as we go about our days. This limited but critical degree of privacy, this barrier between normalcy and the Orwellian dystopia that is becoming reality in some parts of the world, is at risk of being eliminated.

Facial recognition technology, the ability to create a visual biometric “fingerprint” of any person, makes it theoretically possible to instantly identify anyone, anywhere. It has the ability to eliminate the privacy that comes from anonymity once and for all.

For this to happen, the technology would have to be combined with a massive trove of identifiable photographs such as those found spread across the internet. The capacity to do this exists – but companies with the capability to create a mass surveillance facial recognition application have declined to do so. Compl. ¶¶ 14-17. They knew that this would be a step too far. This would be immoral. It would be wrong.

Defendant Clearview AI, a company founded by a technological whiz whose previous endeavors reportedly involved creating software designed to bypass security and steal credentials, has done what no other business was willing to try. It has trolled the internet for billions of photographs, reportedly stealing them from

social media pages and other sites. It has extracted the biometric “fingerprints” of specific individuals from these photographs to create a massive surveillance database. It has probed us, mapped us, and sold us.

Clearview’s app was made available to hundreds or possibly thousands of persons and entities, including foreign countries. Their customers were major businesses from retailers to casinos to health clubs, who were more than happy to use the app as long as no one knew they were doing it. Clearview now claims to be limiting such usage to law enforcement, but it has provided no reason to trust that this policy is true now or that it will continue once Clearview is out of the spotlight.¹

An unknown number of Vermonters are in this database. Not a single one consented to be there. Worse yet, their *children* have been caught in this net as well, and there is no escape from it. We have been forced to be part of an involuntary lineup every time some unscrupulous person or business probes the Clearview database.

By this motion, the Attorney General of Vermont says, “No more.” Clearview’s acts violate Vermont’s Consumer Protection Act and its prohibition against unfair and deceptive acts and practices, as well as Vermont’s Fraudulent Acquisition of Data Law. Clearview’s acts are unethical, immoral, and against all

¹ Even if Clearview somehow limited its app solely to U.S. law enforcement agencies, there would still need to be appropriate safeguards such as appropriate data security and consumer consent, which are currently not in place.

social norms and policies. The State urges that the people of Vermont immediately be set free from Clearview's dystopian surveillance database.

The matter cannot wait any longer. Clearview continues to expand and sell its app to more and more entities. There is also an immediate threat to safety, especially since Clearview was already targeted and breached by hackers. And Clearview cannot be trusted to ensure adequate safeguards are in place to prevent misuse and abuse, especially considering the risk to children of access to their photos.

In sum, Clearview's conduct is unprecedented in our society, it is a "breach of social norms," *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 150 (3d Cir. 2015), and it violates Vermont law. The State seeks a preliminary injunction at this time to immediately cease Clearview's collection of Vermonters' photos, and most importantly, to remove Vermonters' photos, especially those of Vermont children.

Background and Facts

Clearview AI is a small startup technology company. Affidavit of AJ Van Tassel ¶ 7, Exhibit 4 (hereafter "Van Tassel Ex. ___"). Clearview uses and sells a proprietary facial recognition technology as applied to a database of photographs that it collected through screen scraping. Compl. ¶ 24. Clearview's owner is Hoan Ton-That, a California resident with a history of allegedly developing spurious "phishing" technology in order to send "spam." Compl. ¶¶ 26-28; Van Tassel Ex. 5.

Clearview Collects and Stores 3,000,000,000 Photos

Clearview used a technological process known as “screen scraping” to automatically gather approximately three billion online photographs. Van Tassel Aff. ¶ 6; Van Tassel Ex. 3. “Screen scraping” refers to using an automated process, sometimes called a “spider” or “crawler,” to mass-download information from internet websites. *See, e.g., TravelJungle v. Am. Airlines, Inc.*, 212 S.W.3d 841, 847 (Tex. App. 2006) (“Screen-scraping software sends out electronic robots, spiders, or other automated scraping devices across the Internet to enter and search targeted . . . websites, . . . and extracts proprietary [data] from the sites.”); Sean O'Reilly, *Nominative Fair Use and Internet Aggregators: Copyright and Trademark Challenges Posed by Bots, Web Crawlers and Screen-Scraping Technologies*, 19 Loy. Consumer L. Rev. 273, 277 (2007) (“Screen scraping’ refers to a process whereby content can be pulled off a website[] on the internet using robot/crawler scripts.”) (hereafter, referred to as “scraping”). This technique bypasses the intended use and limitations of the websites and their publishers. Compl. ¶¶ 39, 43-44.

Clearview used scraping technology to gather photos from countless internet sites including Google, Facebook, Twitter, YouTube, Venmo, and LinkedIn, among others. Van Tassel Ex. 3. Many of these websites contain terms of service with prohibitions on screen scraping and implement technology to attempt to prevent screen scraping. *Id.* Clearview’s scraping violated these contracts and terms of service and bypassed those technological protections. Compl. ¶ 43. The following

examples of several noteworthy websites' terms of service all expressly prohibit what Clearview did:

- Facebook: “You may not access or collect data from our Products using automated means (without prior permission) or attempt to access data you do not have permission to access” and “You will not engage in Automated Data Collection without Facebook’s express written permission.”²
- Google: “You may not copy, modify, distribute, sell, or lease any part of our Services” and “You may not use content from our Services unless you obtain permission from its owner or are otherwise permitted by law.”³
- Twitter: “you may not . . . access or search or attempt to access or search the Services by any means (automated or otherwise) other than through our currently available published interfaces that are provided by Twitter” and explicitly stating that “scraping the Services without the prior consent of Twitter is expressly prohibited.”⁴
- YouTube: a person may not “access the Service using any automated means (such as robots, botnets or scrapers) except . . . with YouTube’s prior written permission” and may not “collect or harvest any information that might identify a person, unless permitted by that person.”⁵
- LinkedIn: a user agrees that they “will *not*. . . use software, devices, scripts, robots or any other means or processes (including crawlers, browser plugins and add-ons or any other technology) to scrape the

² Facebook Terms of Service, section 3, item # 3, *available at*: <https://www.facebook.com/terms.php> (last visited Mar. 9, 2020); *and* Facebook “Automated Data Collection Terms” at ¶ 2, *available at*: https://www.facebook.com/apps/site_scraping_tos_terms.php (last visited Mar. 9, 2020);

³ Google Terms of Service, *available at*: <https://policies.google.com/terms> (last visited Mar. 9, 2020)

⁴ Twitter User Agreement, section 4, *available at*: <https://twitter.com/en/tos> (last visited Mar. 9, 2020).

⁵ YouTube Terms of Service, “Use of Service,” ¶¶ 3-4, *available at*: <https://www.youtube.com/static?template=terms> (last visited Mar. 9, 2020).

Services or otherwise copy profiles and other data from the Services.”⁶
[emphasis in original]

- Venmo: “you must not . . . use any robot, spider, or other automatic device, or manual process to monitor or copy our websites without our prior written permission”; “you must not . . . infringe our or any third party’s . . . rights of publicity or privacy”; and “you must keep” all Venmo customer information “confidential and only use it in connection with the Venmo services.”⁷

Clearview violated all of the above contractual terms of service. Clearview also did not obtain any rights to the photos it collected. Compl. ¶¶ 38, 41-42.

Further, the subjects of many of these photos never consented to have them posted online at all, and certainly not to be collected in the way Clearview has. *See, e.g.*, Compl. ¶ 45 (noting that many photos on the internet are uploaded by third parties, including photos taken well before the internet’s creation). Based on the fact that Clearview’s owner has a reported history of using phishing technologies, it is also possible that Clearview may have actively bypassed the privacy settings set by users and collected photos that were never available for viewing or sharing. Compl. ¶¶ 27-28, 46.

Clearview Collects and Stores Photos of Minors

Clearview’s scraping did not distinguish among adults or children. But Clearview knows that it has photos of children in its database, as it acknowledged in its January 2020 filing with Vermont’s Data Broker Registry. Van Tassel Ex. 2.

⁶ LinkedIn User Agreement, section 8.2, *available at*: <https://www.linkedin.com/legal/user-agreement> (last visited Mar. 9, 2020).

⁷ Venmo User Agreement, “Restricted Activities,” *available at*: <https://venmo.com/legal/user-agreement/> (last visited Mar. 9, 2020).

(answering “yes” to the question: “Does the data broker have actual knowledge that it possesses the brokered personal information of minors?”). Additionally, Clearview stated that “[w]e actively work to remove all” photos of minors from California, thus further indicating that Clearview collected children’s photos. *Id.*

Clearview Uses Facial Recognition AI to Match People

In addition to collecting and storing billions of photos, Clearview developed a facial recognition algorithm. Van Tassel Ex. 4. Users of Clearview’s app can upload a photo of an individual and the Clearview technology will return, in real time, all of the photos in its database in which that person appears. The person could be in a crowd, the background, or even a reflection in a mirror. Clearview does this by mapping the person’s facial features to create a biometric “fingerprint” of the person being searched, and then finds that fingerprint in other photos. Compl. ¶¶ 11-13. Clearview returns to the user an indicator of where that photo exists on the internet. Combined with other readily available tools or data sources, there is no limit to obtaining other identifiable and personal details like addresses, locations, relatives, friends and associates, etc. Compl. ¶ 15. For example, using this app, one could go to a public park, a shopping center, or a protest, and then photograph individuals and instantly find their LinkedIn profiles. In fact, The New York Times recently reported that wealthy investors were using the app for exactly this purpose. Van Tassel Ex. 9.

Facial recognition technology in general is highly controversial. It is often inaccurate, particularly with respect to persons of color, and it is so new and

emergent that there are few or no legal safeguards and protections against abuse and misuse. See Compl. ¶¶ 14-18. For example, the National Institute of Standards and Technology of the U.S. Department of Commerce (NIST) is the federal agency that benchmarks facial recognition algorithms. NIST released a report in December 2019 which found that the technology is, across the board, inaccurate with regard to African Americans and Asians at a rate 10-100 times that of Caucasians. Compl. ¶ 19. Many entities even refuse to use facial recognition technology for the purposes Clearview has. See Compl. ¶¶ 16-17; 21-22 (Google has refrained from developing facial recognition technology for mass use by the public; several states, municipalities, and agencies have banned it or are considering bans).

Clearview Sells its Technology to Whomever Clearview Decides

Clearview claims that its app is not publicly available. Van Tassel Ex. 11. Clearview currently states that its app is expressly for law enforcement to conduct their own searches. *Id.* (claiming that Clearview's app can help "solve their toughest cases").

Despite these claims, Clearview's app is not in fact solely limited to law enforcement. As a result of a recent data breach in which Clearview's entire customer list was stolen, Clearview's customers are now known and they are wide-reaching. According to news reports, Clearview's customers included some of the largest U.S. businesses such as: Best Buy, Macy's, Kohl's, Walmart, Albertsons, Home Depot, Rite Aid, AT&T, Verizon, and T-Mobile. Van Tassel Ex. 7. They also included banks (Wells Fargo and Bank of America) and other large organizations

(Las Vegas Sands Casino, Equinox Fitness, Madison Square Garden, the NBA, and more than 50 universities). *Id.* Clearview has even provided its app to other countries like Saudi Arabia and the United Arab Emirates. *Id.* Further, according to a news report, Clearview also gave access to its app to the company's investors, clients and friends. Van Tassel Ex. 9. As The New York Times reported, the app was a "perk" for investors and a "plaything of the rich"; as one investor stated, people would "use it on themselves and their friends to see who they look like in the world . . . It's kind of fun for people." *Id.*

In marketing its app, Clearview pushes the unrestricted nature of its technology. In one promotional email sent by Clearview: Clearview recommended searching "friends or family [o]r a celebrity"; Clearview told users of the app "to run wild with your searches"; and Clearview claimed that your searches "are **always** private" and "**never** stored" by Clearview. Van Tassel Ex. 8 (emphasis in original). This last statement is particularly problematic because a best practice would typically require the storage and audit of searches. *See, e.g., The Perpetual Line-up: Unregulated Police Face Recognition in America*, Georgetown Law Center on Privacy & Technology (Oct. 18, 2016) at 118.⁸

Clearview Misrepresents its Product

Clearview makes several materially false and misleading claims about its product. *First*, Clearview has a Privacy Policy and claims that members of the public have express "data protection rights," including rights to remove and erase

⁸ Available at: www.perpetuallineup.org (hereafter "*The Perpetual Line-up Report*") (last visited Mar. 9, 2020).

their photos from the app, and that Clearview will comply with those requests. Van Tassel Ex. 10. In fact, these rights are subject to a limitation by Clearview, which states that it will only honor a deletion request in jurisdictions where there is a regulation requiring them to do so. *Id.* For example, the “data protection rights” cited by Clearview are those conferred upon citizens in the European Union. There is no United States federal law that provides these rights, and the only State law that provides any similar explicit rights exists in California, and only applies to California citizens. Compl. ¶¶ 57-58. Thus, Clearview’s claims—made to assuage privacy fears—are materially false and misleading with respect to all non-California U.S. residents, including Vermonters. *Id.* Further to this point, Clearview also states that it “actively work[s]” to remove images of minors from California and that it can “process[] all opt-out requests.” Van Tassel Ex. 2. However, this too is false. To the State’s knowledge, Clearview currently has no such capability to detect and remove minors’ photos or even any photos based on age or geographic location. Compl. ¶ 51.

Second, Clearview claims that it “secure[s] all personal information that we store on computer servers in a controlled, secure environment, protected from unauthorized access, use or disclosure” and that it uses “appropriate physical, technical and organizational measures.” Van Tassel Ex. 10. To date, Clearview has not demonstrated to the Attorney General’s Office or otherwise that it has implemented reasonable data security measures. Compl. ¶ 63. In fact, two weeks prior to this filing, Clearview suffered a significant data breach. Van Tassel Ex. 6;

Affidavit of Jay Bailey, Exhibit 1. Clearview has created a misimpression that its data is being stored with reasonable data security, which is materially false and misleading. *Id.* See also Compl. ¶¶ 61-65.

Finally, Clearview has made a number of other claims that reflect on its general lack of candor and trustworthiness, which leads to further skepticism of its other promises. These include claims that its product is only used by law enforcement and that it enforces a code of conduct with regard to that use. Van Tassel Ex. 12 (Clearview's code of conduct states that the app is for "legitimate law enforcement and security purposes" and not "for personal purposes or any purposes which are not authorized and directed by the user organization's supervisors."). Despite this self-described limitation, Clearview markets its app with no restrictions, encouraging users "to run wild" with their searches and highlighting how searches are "never stored." Van Tassel Ex. 8.

Clearview also claims that its product is highly accurate, with matching accuracy of 98-99% regardless of demographics. Compl. ¶¶ 71-72. This claim, which Clearview asserted was based on a methodology used by the ACLU, was actually criticized by the ACLU as "absurd on many levels." Compl. ¶ 72. Clearview also has not submitted its algorithm to the NIST Face Recognition Vendor Test, which is the only public benchmark for determining the accuracy of facial recognition software. Compl. ¶ 73. Although Clearview states that its app helps solve crimes generally, Clearview made specific claims of solving crimes in New York that were subsequently debunked. Compl. ¶¶ 74-75 (claiming that Clearview's app solved two

assaults and a suspected terrorist attack in New York City, which was disputed by the NYPD).

In sum, Clearview's business is unlawful in Vermont. Vermonters' photos have been unlawfully scraped by Clearview and are currently in Clearview's database, being secretly searched by anyone who purchased or obtained Clearview's app. This includes children in Vermont. As outlined in detail below, an immediate injunction is warranted to remedy this unlawful conduct.

Argument

I. Applicable Standards for an Injunction

A. An Injunction is Authorized by Statute

Title 9 V.S.A. § 2458(a) empowers the Attorney General to seek a preliminary or permanent injunction to restrain violations of the Vermont Consumer Protection Act ("CPA" or "the Act"). The statute articulates two factors for requesting an injunction – reasonable belief that the Act has been violated, and reasonable belief that proceedings would be in the public interest:

Whenever the attorney general . . . has reason to believe that any person is using or is about to use any method, act or practice declared by section 2453 of this title to be unlawful . . . and that the proceedings would be in the public interest, the attorney general . . . may bring an action in the name of the state against such person to restrain by temporary or permanent injunction the use of such method, act or practice The courts are authorized to issue temporary or permanent injunctions to restrain and prevent violations of this chapter

9 V.S.A. § 2458(a).

Per section 2458(a), the State may seek either a temporary or permanent injunction. At this time, the State seeks a preliminary injunction. A preliminary injunction is necessary now because Clearview's conduct is ongoing and Vermonters' substantial privacy and safety interests are being violated. Clearview is a recently launched company that is expanding. Van Tassel Ex. 4. In fact, Clearview's conduct and harms continue to mount in real time. As of two weeks ago, Clearview had a significant data breach. Van Tassel Ex. 6; Bailey Ex. 1. Thus, a preliminary injunction is also necessary to prevent the ongoing threat of an illegal data breach resulting in the acquisition of Vermonters' private images and facial recognition fingerprints by unscrupulous third parties for uses ranging from fraud to identity theft to espionage. Compl. ¶ 67.

For the reasons set forth below, the State has sufficient evidence to prove the standards for a preliminary injunction.

B. Legal Standards for a Statutory Injunction

"This is a case in which an injunction is expressly authorized by statute."

Minnesota ex rel. Hatch v. Sunbelt Commc'ns & Mktg., 282 F. Supp. 2d 976, 979 (D. Minn. 2002) (upholding injunction by Minnesota Attorney General for violations of Telephone Consumer Protection Act). *See also Chick Kam Choo v. Exxon Corp.*, 486 U.S. 140, 146 (1988) (distinguishing injunctions that are "expressly authorized by statute").

Accordingly, in deciding whether to grant a motion for a preliminary injunction that is requested pursuant to statute, this Court need only consider the

action's likelihood of success on the merits.⁹ See *United States v. Estate Pres. Servs.*, 202 F.3d 1093, 1098 (9th Cir. 2000) (noting "the traditional requirements" for injunctive relief "need not be satisfied" where injunction is expressly authorized by statute); *Henderson v. Byrd*, 133 F.2d 515, 517 (2d Cir. 1943) ("The contention that the plaintiff failed to prove the existence of the usual equitable grounds for relief, such as irreparable damage, is plainly irrelevant. Where an injunction is authorized by statute, it is enough if the statutory conditions are satisfied."); *Env'tl. Def. Fund v. Lamphier*, 714 F.2d 331, 338 (4th Cir. 1983) (where a statute authorizes injunctive relief for its enforcement, plaintiffs need not plead and prove irreparable injury); *United States v. Weingold*, 844 F. Supp. 1560, 1573 (D. N.J. 1994) ("Proof of irreparable harm is not necessary for the Government to obtain a preliminary injunction."); *United States v. White*, 769 F.2d 511, 515 (8th Cir. 1985) ("When an injunction is explicitly authorized by statute, proper discretion usually requires its issuance if the prerequisites for the remedy have been demonstrated and the injunction would fulfill the legislative purpose."); *United States v. City and County of San Francisco*, 310 U.S. 16, 30-31 (1940) (no balancing of the equities necessary where government seeks injunction to implement federal legislative policy).

Further, under the doctrine of statutory injunctions, it is presumed that statutory injunctions are in the public interest. "The principle underlying the

⁹ The traditional factors for granting a motion for preliminary injunction are: (1) the threat of irreparable harm to the movant, (2) the potential harm to the other parties, (3) the likelihood of success on the merits, and (4) the public interest. *In re J.G.*, 160 Vt. 250, 255-56 n.2 (1993); see also 11A Wright, Miller & Kane, Federal Practice and Procedure: Civil 2d § 2948 at 131-33 (1995).

willingness of the courts to issue statutory injunctions to public bodies to restrain violations of a statute is that harm to the public at large can be presumed from the statutory violation alone.” *People ex rel. Hartigan v. Stianos*, 475 N.E.2d 1024, 1027-28 (Ill. App. Ct. 1985). *See also Webster v. Milbourn*, 759 S.W.2d 862, 864 (Mo. Ct. App. 1988) (potential harm to the public is presumed once court finds that defendant has engaged in unlawful trade practices); *State v. Fonk’s Mobile Home Park & Sales*, 343 N.W.2d 820, 823-25 (Wis. Ct. App. 1983) (statutory injunction may be issued under consumer protection statute without proof of future harm).

Therefore, the only factor for analysis is whether the State can show a likelihood of success that Clearview violated Vermont law. As discussed below, based on the evidence to date, Clearview has violated the CPA in numerous ways as well as Vermont’s Fraudulent Acquisition of Data Law. Thus, the Motion for a Preliminary Injunction should be granted.

II. Overview of Vermont Consumer Protection Act

The CPA prohibits “unfair or deceptive acts or practices in commerce.” 9 V.S.A. § 2453(a). The CPA is a remedial statute, to be interpreted liberally to accomplish its purpose of protecting consumers. *Carter v. Gugliuzzi*, 168 Vt. 48, 716 52, 716 A.2d 17, 21 (1998) (“The express statutory purpose of the Act is to protect the public against unfair or deceptive acts or practices Its purpose is remedial, and as such we apply the Act liberally to accomplish its purposes.”) (internal quotation marks omitted).

In interpreting the Act, Vermont courts are “guided by the construction of similar terms contained in . . . the Federal Trade Commission [FTC] Act and the courts of the United States.” 9 V.S.A. § 2453(b).

Under the CPA, “unfairness” and “deception” are two separate prohibitions. *Dernier v. Mortgage Network, Inc.*, 195 Vt. 113, 87 A.3d 465, 2013 VT 96, ¶ 55 (“‘Unfair’ acts and ‘deceptive’ acts each have their own tests”); *Orkin Exterminating Co., Inc. v. FTC*, 849 F.2d 1354, 1367 (11th Cir. 1988) (“[T]he unfairness doctrine differs from, and supplements, the prohibition against consumer deception.”). Each is discussed below.

A. Unfairness

The Vermont Supreme Court has recognized three independent criteria for determining whether or not a practice is unfair:

“(1) whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise – whether, in other words, it is within at least the penumbra of some common-law, statutory, or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; (3) whether it causes substantial injury to consumers”

Christie v. Dalmig, Inc., 136 Vt. 597, 601, 396 A.2d 1385, 1388 (1979) (quoting *FTC v. Sperry & Hutchinson Co.* (“*Sperry*”), 405 U.S. 233, 244 n.5 (1972)).

It is not necessary that all three criteria be met so long as the practice is “exploitive or inequitable” or “is seriously detrimental to consumers or others.” *Sperry*, 233 at 244 n.5. See also *Christie*, 136 Vt. at 601 (noting that there is an open question as to “whether one or all of these factors must be present”); *State of Vermont v. CSA-Credit Solutions of Am., LLC & Doug Van Arsdale*, Dec. and Order:

Mot. for Summ. J., at 7 (Vt. Super. Ct. March 5, 2012) (inserting an “or” into the three-part *Sperry* standard articulated in *Christie*) (attached as Ex. A hereto).

B. Deception

In Vermont, a deceptive act or practice contains three elements: “(1) there must be a representation, omission, or practice likely to mislead consumers; (2) the consumer must be interpreting the message reasonably under the circumstances; and (3) the misleading effects must be material, that is, likely to affect the consumer’s conduct or decision regarding the product.” *Carter*, 168 Vt. at 56 (consumer stated claim of deception where real estate agent failed to disclose material facts).

The third element of deception, materiality, is measured by an objective standard, “premised on what a reasonable person would regard as important in making a decision.” *Carter*, 168 Vt. at 56. The federal courts and the FTC “apply a general presumption of materiality.” *Id.* For example, “where the seller knew, or should have known, that an ordinary consumer would need omitted information to evaluate the product or service, or that the claim was false, materiality will be presumed because the manufacturer intended the information or omission to have an effect.” *Id.* (quoting *In re Cliffdale Assocs., Inc.*, No. 9156, 1984 WL 565319, at *49 (FTC Mar. 23, 1984)).

Materiality is also presumed where a claim is express. *See Carter*, 168 Vt. at 56. Similarly, claims or omissions are automatically deemed material if they involve “areas with which the reasonable consumer would be concerned.” *In re Cliffdale Assocs.*, 1984 WL 565319 at *49.

III. Defendant Clearview Has Committed Unfair and Deceptive Acts

Defendant collects and stores facial-recognition images of Vermonters, including children, without their consent and without sufficient guardrails to protect this highly sensitive data. Defendant then sells this data to third parties, for the express purpose of facilitating unrestricted surveillance. This constitutes unfair and deceptive conduct in several ways:

- (a) it violates consumers' reasonable expectation of privacy (Compl., Count I);
- (b) it violates internet contracts and terms of service (Compl., Count I);
- (c) it fails to provide adequate data security under Vermont law (Compl., Count I);
- (d) it is deceptive regarding its privacy protections, its data security, and the uses and accuracy of its product (Compl., Count II);
- (e) it is immoral, unethical, oppressive or unscrupulous (Compl., Counts I-III); and
- (f) it fraudulently acquires data in violation of Vermont law (Compl., Count III).

A. Defendant's conduct is unfair because it violates consumers' right and expectation of privacy.

As set forth above, an unfair act includes one that "offends public policy as it has been established by statutes, the common law, or otherwise – whether, in other words, it is within at least the penumbra of some common-law, statutory, or other established concept of unfairness." *Christie*, 136 Vt. at 60. Defendant's

conduct is first unfair under the CPA (Count I of the Complaint) because it offends the policies and principles as expressed under the laws of privacy.

1. *Right to privacy generally.*

Vermonters have a substantial and fundamental right to privacy that protects their likenesses and images, and precludes universal surveillance from a private company that sells such services. This right to privacy is grounded in the common law. See *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 & n. 15 (1989) (recognizing the common law's protection of a privacy right); *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469, 488 (1975) (noting that a right to privacy had been recognized at common law in the majority of American jurisdictions).

“The manifold nature of what is loosely termed ‘the right to privacy’ is well established.” *Birnbaum v. United States*, 588 F.2d 319, 323 (2d Cir. 1978). In *Birnbaum*, the Second Circuit firmly established “the right of seclusion to be free from unreasonable intrusion by another” and reviewed the Restatement on Torts, noting that the “common” thread of all privacy actions is that that “each represents an interference with the right of the plaintiff ‘to be let alone.’” *Id.* (quoting Dean W. Prosser, *The Law of Torts*, at 804 (4th ed. 1971)).

Vermonters enjoy a common law right to anonymity and the right to be left alone. *Denton v. Chittenden Bank*, 163 Vt. 62, 68–69, 655 A.2d 703, 707 (1994) (“The right of privacy is the right to be left alone.”). “Anonymity is an important element of the right of privacy and the related constitutional right to peaceably

assemble.” Giorgio Bovenzi, *Liabilities of System Operators on the Internet*, 11 Berkeley Tech. L.J. 93, 103 (1996). *See also id.* (explaining that “[t]he Internet offers a practical opportunity for assembling and communicating in anonymity” and noting that “the protection of anonymity is rooted in both freedom of speech and the right to privacy.”).

Vermonters also have a right to privacy from a penumbra of constitutional protections under the First and Fourth Amendments to the United States Constitution and Article 11 of the Vermont Constitution. *See also McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 357 (1995) (striking law that required pamphlets to include a name and address, and discussing the “right to anonymity” under the First Amendment).

Finally, the State of Vermont has an interest in protecting the privacy of its consumers. “The government’s interest in preventing any intrusions on individual privacy is substantial.” *State v. VanBuren*, 2018 VT 95 ¶ 57, 214 A.3d 791, 811 (Vt. 2019), as supplemented (June 7, 2019). “[T]he United States Supreme Court stated that the government has a substantial interest in protecting the public’s right to privacy.” *Minnesota ex rel. Hatch*, 282 F. Supp. 2d at 982 (citing *Edenfield v. Fane*, 507 U.S. 761, 769 (1993) (“the protection of potential clients’ privacy is a substantial state interest.”)).

2. *The right to privacy develops with technology.*

The right to privacy has been inextricably linked to the development of technology. Starting from an 1890 law review article by Samuel D. Warren and

Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890), these authors described the very same issue presented in this case:

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right “to be let alone.” Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house-tops. For years there has been a feeling that the law must afford some remedy for *the unauthorized circulation of portraits of private persons*

VanBuren, 2018 VT 95, ¶ 39 (emphasis added and citation omitted). *See also id.*

(noting that “[w]e describe this article in detail because it is frequently cited as a critical catalyst to the development of right-to-privacy law in this country”). Thus, even in 1890, Justice Brandeis warned against “the unauthorized circulation of portraits of private persons,” which is the very harm that Clearview now perpetuates.

Next, society’s reasonable expectation of privacy as it relates to developing technology is often discussed in the Fourth Amendment context. The principles in those cases are instructive here.

For example, in *United States v. Jones*, 565 U.S. 400, 402 (2012), the Supreme Court held that the government’s secret use of a GPS device to track defendant’s vehicle violated the Fourth Amendment. The Court’s holding was premised on the fact that “a reasonable person would not have anticipated” being tracked down by the government using a GPS device. *Id.* at 430. Specifically, “society’s expectation has been that law enforcement agents and others would

not—and indeed, in the main, *simply could not—secretly* monitor and catalogue every single movement of an individual’s car for a very long period.” *Id.* (emphasis added).

Next, in *Carpenter v. United States*, the Supreme Court held that obtaining warrantless cell phone records to track an individual’s location violates Fourth Amendment protections because a person has a reasonable expectation of privacy in their movements. 138 S. Ct. 2206, 2220, 201 L. Ed. 2d 507 (2018). The Court particularly relied on the developing technology of cell phones, “almost [a] feature of human anatomy,” *id.* at 2218, and noted that “[a]s technology has enhanced the Government’s capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to ‘assure [] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.’”) *Id.* at 2214 (citation omitted). *See also id.* at 2223 (the “progress of science . . . does not erode” privacy protections).

These constitutional principles are an important guide in privacy law. *See* Eli A. Meltz, *No Harm, No Foul? “Attempted” Invasion of Privacy and the Tort of Intrusion Upon Seclusion*, 83 *Fordham L. Rev.* 3431, 3437 (2015) (“[d]espite the differences between tort law and constitutional protections of privacy, it is still reasonable to view the interests and values that each protect as connected and related.”). We do not argue here that Vermonters’ Fourth Amendment rights have been violated, as Clearview is not a government entity, merely that Vermonters

have a clear privacy right that is often expressed in Fourth Amendment jurisprudence.

Privacy rights are particularly relevant in the realm of facial recognition technology. For example, the FTC published a white paper in 2012 analyzing the then-emerging technology of facial recognition. FTC, *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies* (Oct. 2012).¹⁰ After collecting input from numerous stakeholders, the Commission concluded that:

- “[T]he use of facial recognition technologies can raise privacy concerns.” [page 7]
- “For example, panelists voiced concerns that databases of photos or biometric data may be susceptible to breaches and hacking.” [page 7]
- “Panelists representing companies that currently use facial recognition technologies similarly acknowledged that there are privacy concerns surrounding the use of these technologies. For example, a Google representative noted the company’s reluctance to implement facial recognition until it had put appropriate privacy protections in place.” [page 7]

Finally, the common law consistently acknowledges the importance of applying the law in order to match technology. As the Restatement of Torts states:

Other forms [of privacy] may still appear, particularly since some courts, and in particular the Supreme Court of the United States, have spoken in very broad general terms of a somewhat undefined “right of privacy” as a ground for various constitutional decisions involving indeterminate civil and personal rights. These and other references to the right of privacy, particularly as a protection against various types of governmental interference and the compilation of elaborate written or computerized dossiers, may give rise to the expansion of the four forms of tort liability for invasion of privacy listed in this Section or the establishment of new forms. Nothing in this Chapter is intended to exclude the possibility of future developments in the tort law of privacy.

¹⁰ Available at: <http://www.ftc.gov/os/2012/10/121022facialtechrpt.pdf>. (hereafter, “*FTC Facing Facts Report*”) (last visited Mar. 9, 2020).

Restatement (Second) of Torts § 652 (1977), cmt. c (emphasis added). Similar to this case, the right to privacy must be recognized against Defendant's elaborate, *computerized* system of collecting photos, without consent, and identifying Vermonters using biometric AI. When the Restatement was drafted in 1977, Clearview's technology existed solely in the realm of (dystopian) science fiction.

Fortunately, the law anticipates such technological developments. *See e.g., Birnbaum*, 588 F.2d at 325–26 (“We are also aware that ‘law does change with times and circumstances, and not merely through legislative reforms.’ A refusal to accept a perceptible trend may be as much a failure to follow state law as a refusal to apply existing precedent because it is somewhat ambiguous.”) (quoting *Bernhardt v. Polygraphic Co.*, 350 U.S. 198, 209, 76 S.Ct. 273 (1956) (Frankfurter, J., concurring)). *See also* Robert D. Lang & Lenore E. Benessere, *Alexa, Siri, Bixby, Google’s Assistant, and Cortana Testifying in Court*, 74 J. Mo. B. 20, 22–23 (2018) (discussing the emerging AI technology of voice recognition: “[r]emembering Judge Cardozo’s remark that ‘law never is, but is always about to be,’ and Chief Justice John Roberts’ comment that ‘*advancing technology poses one of the biggest challenges for the Supreme Court*,’ forward thinking attorneys should not shy away from putting these issues before the court, as attorneys and judges . . . together grapple with this new technology”) (emphasis added).

3. *The right to privacy is an actionable right.*

An invasion of one's privacy is an actionable tort in Vermont. “Invasion of privacy is a substantial, intentional intrusion upon the solitude or seclusion of

another, or upon his private affairs or concerns, which would be highly offensive to a reasonable person.” *Harris v. Carbonneau*, 165 Vt. 433, 439, 685 A.2d 296, 300 (1996) (citing *Hodgdon v. Mount Mansfield Co.*, 160 Vt. 150, 162, 624 A.2d 1122, 1129 (1992); Restatement (Second) of Torts §§ 652A, 652B (1977)).

This invasion of privacy is often referred to as “intrusion upon seclusion.” *See, e.g., Weinstein v. Leonard*, 2015 VT 136, ¶ 29, 200 Vt. 615, 628, 134 A.3d 547, 556–57 (2015) (noting that “[i]n order to succeed in a claim for intrusion upon seclusion, a plaintiff must show an ‘intentional interference with [her] interest in solitude or seclusion, either as to [her] person or as to [her] private affairs or concerns, of a kind that would be highly offensive to a reasonable [person].’ The intrusion ‘must be substantial.’”) (quoting *Hodgdon*, 160 Vt. 150 and citing Restatement (Second) of Torts § 652B).

4. *Clearview has engaged in unfair trade practices by violating Vermonters’ right to privacy.*

Here, Defendant’s conduct is an unfair act under the CPA because it violates both the spirit and letter of privacy law. It violates Vermonters’ common law rights to privacy, including an intrusion upon Vermonters’ seclusion. All three elements of the tort claim are satisfied.

First, Defendant knowingly and intentionally accesses consumers’ photos that are available on the internet. There is no mistake about Defendant’s scienter of its conduct.

Second, Defendant’s conduct is substantial. Vermonters, including children, are now in a database (controlled by Clearview) where they can be readily

identified using a simple, real-time app. Collecting, storing, and making available three billion photos, including children, without consent, is not merely “a handful of minor offenses.” *Weinstein*, 2015 VT 136 at ¶ 32, 200 Vt. at 629, 134 A.3d at 557 (noting that “a handful of minor offenses are insufficient to constitute a tortious intrusion upon seclusion” and holding that two encounters with harassing neighbor was insufficient for privacy claim). Similarly, Defendant’s business is not “routine commercial behavior.” *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986 (Ca. 2011). In *Folgelstrom*, the California Court of Appeals affirmed the dismissal of a constitutional privacy claim because “the supposed invasion of privacy essentially consisted of [defendant] obtaining plaintiff’s address without his knowledge or permission, and using it to mail him coupons and other advertisements.” The court held that “[t]his conduct is not an egregious breach of social norms, but routine commercial behavior.” *Id.*

Contrary to the above cases, Defendant’s conduct is no small or mundane commercial activity. Rather, it is a pervasive and wide-sweeping collection of our photos without consent and in violation of various terms of service by social media companies, in order to facilitate our identification by third parties, by law enforcement, by numerous private individuals and businesses, and even by foreign governments. Such action has never before been attempted in the United States, and consumers reasonably expected that it never would be attempted. *See, e.g., supra* note 10, *FTC Facing Facts Report* at 7 (Google stated that the company would

not use facial recognition technology “until it had put appropriate privacy protections in place.”).

Third, Defendant’s conduct is highly offensive to a reasonable person. Vermonters did not consent to having their photos collected, stored, and searched without restrictions by wealthy investors or law enforcement or foreign countries or Walmart, Kohl’s, Rite Aid, etc. *See Van Tassel Exs. 7 and 9*. Vermonters also did not consent to having their photos searched in order to match and identify them by the countless individuals or entities who possess Clearview’s app. A reasonable person holds closely their anonymity and does not waive this privacy interest by posting to social media sites that expressly protect the privacy of their photos. This privacy interest is heightened when it comes to children because they cannot consent to their data being used, and are now effectively in Clearview’s database forever. *See Compl. ¶ 49-51*. Further, their data could be compromised and exploited.

That third parties can access and identify who we are by uploading pictures to Clearview’s database and engage in universal surveillance goes to the very core of privacy and our expectation that we may remain anonymous and left alone. This is particularly so in the realm of advancing technology and society’s growing and inescapable presence on the internet.

For example, courts have found privacy violations when companies can monitor or identify an individual or that individual’s online habits. *See, e.g., Cooper v. Slice Techs., Inc.*, No. 17-CV-7102 (JPO), 2018 WL 2727888, at *3

(S.D.N.Y. June 6, 2018) (noting that “unauthorized accessing and monitoring of plaintiffs’ web-browsing activity implicates harms similar to those associated with the common law tort of intrusion upon seclusion”); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 153 (3d Cir. 2015) (reversing district court’s dismissal of privacy claims against Google for secretly tracking user websites, and holding that a “reasonable factfinder could conclude that” Google’s use of “cookies” was “deceitful” and “marks the serious invasion of privacy contemplated by California law.”); *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1091 (N.D. Cal. 2018) (finding that Uber’s collection of home addresses invaded plaintiff’s privacy, but ultimately dismissing claim where no facts alleged as to what Uber did with plaintiff’s home address, and citing *Williams v. Superior Court*, 3 Cal. 5th 531, 554, 398 P.3d 69, 85 (2017), which held that “home contact information is generally considered private.”).

More recently, the Ninth Circuit decided a similar privacy case against Facebook for its use of facial recognition technology. *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1269 (9th Cir. 2019), *cert. denied*, No. 19-706, 2020 WL 283288 (U.S. Jan. 21, 2020). In upholding a class action based on Illinois’ new state law on biometric privacy protection, the court found that Facebook used biometric data without consumers’ consent to create a facial recognition algorithm for “tagging” photos on Facebook. *Id.* at 1273. The court first noted the critical link between privacy and technology: “[a]s in the Fourth Amendment context, the facial-recognition technology at issue here can obtain information that is ‘detailed,

encyclopedic, and effortlessly compiled,' which would be almost impossible without such technology." *Id.* Thus, the court "conclude[d] that the development of a face template using facial-recognition technology without consent (as alleged here) invades an individual's private affairs and concrete interests. Similar conduct is actionable at common law." *Id.*

On the other hand, if data is anonymous or of a general nature, courts typically do not find privacy violations. *See, e.g., Mount v. PulsePoint, Inc.*, 684 F. App'x 32, 35 (2d Cir. 2017) (court rejected unfair and deceptive claims for a website that collected only anonymous browser data and noting that a privacy "injury has been recognized only where confidential, individually identifiable information—such as medical records or a Social Security number—is collected without the individual's knowledge or consent."). *See also In re Google Location History Litig.*, No. 5:18-CV-05062-EJD, 2019 WL 6911951, at *10 (N.D. Cal. Dec. 19, 2019) (rejecting class action claim against Google Maps for tracking geolocation of users, including minors, and holding that "[a] person's general location is not the type of core, value, informational privacy explicated in [other California precedent].")

Here, Clearview's database is by no means anonymous or of a general nature. It is highly specific and personal. Its express purpose is to facilitate the identification of every person searched. Clearview did not merely copy our photos. Clearview created a biometric AI that assigns a unique identifier to those photos *for identification purposes*. It is a map of who we are, based on our internet

photos, and it is available to anyone Clearview decides to sell to. This carries enormous privacy implications. *See Patel*, 932 F.3d at 1269 (noting that “[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information, because while social security numbers can be changed if compromised by hackers, biometric data are biologically unique to the individual, and once compromised, the individual has no recourse, [and] is at heightened risk for identity theft”) (quotations omitted).

Defendant’s conduct is thus highly offensive and a “breach of social norms.” *Google Cookie Placement Litig.*, 806 F.3d at 150. The offensiveness is far greater when considering that children are included in Clearview’s app. Indeed, far less offensive conduct has been found to be a privacy violation of minors. For example, in *McDonald v. Killoo ApS*, 385 F. Supp. 3d 1022, 1029 (N.D. Cal. 2019), the California federal district court upheld privacy claims under California’s Unfair Competition Law against a gaming app for collecting user data on children to monitor and track their activities for the purpose of targeted advertising. In allowing the consumer protection claim (based on privacy interests) to go forward, the court noted that: “Current privacy expectations are developing, to say the least, with respect to a key issue raised in these cases -- whether the data subject owns and controls his or her personal information, and whether a commercial entity that secretly harvests it commits a highly offensive or egregious act.” *Id.* at 1035. The court concluded that the gaming app “breaches social norms” by

collecting minors' data and went far beyond "routine commercial behavior." *Id.* at 1038.

Similarly, the FTC has also brought actions against internet companies that track children for purposes of targeted advertising. *See FTC v. InMobi Pte Ltd*, No. 3:16-cv-3474 (N.D. Cal. June 22, 2016) (Singapore-based mobile advertising company InMobi paid \$950,000 in civil penalties to settle Federal Trade Commission charges that it secretly tracked millions of consumers', including children's, use of websites for purposes of geo-targeted advertising).¹¹

The same analysis applies here. As in *McDonald* and *InMobi*, Clearview is secretly harvesting identifiable information of minors; here their pictures. This conduct is far more offensive than merely collecting the data for advertising purposes. Facial recognition technology for purposes of matching and identification has far more consequences and intrusions into privacy for children than mere advertising. For example, in 2012, the FTC warned of the very dangers that Clearview now perpetuates:

Social networks could identify non-users of the site – *including children* – to existing users, by comparing uploaded images against a database of identified photos. Although staff is *not aware* of companies currently using data in these ways, if they begin to do so, *there would be significant privacy concerns*.

Supra note 10, *FTC Facing Facts Report* at 8 (emphasis added).

In 2012, the FTC was "not aware of companies using data" in the exact way Clearview now does. But even then, the FTC warned of "significant privacy

¹¹ Available at: <https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked> (last visited Mar. 9, 2020).

concerns,” especially for children. *Id.* In short, the FTC’s prescient statement is the exact warning bell that now tolls and thus warrants injunctive relief. *See also Supra* note 8, *The Perpetual Line-up Report* at 4 (“Real-time face recognition will redefine the nature of public spaces. It should be strictly limited.”).

The fact that Clearview may claim that it only uses photos from the internet that were not restricted would not change the analysis. *See, e.g., Gill v. Hearst Pub. Co.*, 40 Cal. 2d 224, 253 P.2d 441 (1953), where California’s Supreme Court rejected a privacy claim where Harpers’ Bazaar photographed and then published a family sitting in a park. Here, there is a vast difference between a single photographer who may take *one* photo of you while walking down a public street versus Clearview’s practice of secretly, systematically collecting *all* of your photos on the internet for the purpose of biometric identification for law enforcement surveillance and other commercial purposes. The distinction is critical.

For one, the mere posting of a photo on the internet does not and should not eliminate all privacy related rights. *See Carpenter*, 138 S. Ct. at 2217 (“[a] person does not surrender all [privacy] protection by venturing into the public sphere.”). In *Carpenter*, the Court rejected the argument that an individual voluntarily shares their movements with the cell phone provider and thus loses an expectation of privacy. Even where an individual “has a reduced expectation of privacy in information knowingly shared with another,” the Court held that privacy protections do not “fall[] out of the picture entirely.” *Id.* at 2219. The test

is whether there remains “a legitimate expectation of privacy concerning their contents.” *Id.*

The Supreme Court in *Jones* also anticipated that privacy expectations do not dissipate under the internet. In her lengthy concurrence, Justice Sotomayor wrote that:

More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.

This approach is *ill suited to the digital age*, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.

People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.

[. . .]

I would *not assume that all information voluntarily disclosed to some member of the public for a limited purpose is*, for that reason alone, disentitled to Fourth Amendment protection.

Jones, 565 U.S. at 417–18 (emphasis added).

Although Fourth Amendment cases, the principles from *Jones* and *Carpenter* apply because they relate to society’s overall reasonable expectations of privacy.

Clearview cannot claim that consumers voluntarily disclosed their photos for the purposes for which Clearview now uses them. There is no indication that consumers posted photos with the intent of making them public for everyone, let alone for any user of Clearview’s app to “run wild” with searching them. Van Tassel Ex. 8. Many photos have been posted by third parties and without consent. See Compl. ¶ 45.

Some photos may have been re-posted by users who themselves had no authority or consent to do so, and some are made widely available as a result of human error by the host website. *Id.*

Further, even if some photos were uploaded by users for others to view on a website such as Facebook, consumers still expect that photo to remain on Facebook according to the express terms of service. *See supra* note 8, *The Perpetual Line-up Report* at 20 (one of the “founding principles of privacy” is that “personal data should not be used outside of the stated purposes of the [data system] as reasonably understood by the individual, unless the informed consent of the individual has been explicitly obtained.”) (quotation omitted). *See also Carpenter*, 138 S. Ct. at 2217 & 2219 (“venturing into the public sphere” does not eliminate all privacy expectations; the test is whether there remains “a legitimate expectation of privacy concerning their contents.”).

In this case, consumers have no expectation, or even indication, that their internet photos could now be compiled effortlessly and secretly searched by anyone with access to Clearview’s app, and not just law enforcement, but foreign nations, wealthy investors, celebrities, major businesses, banks, casinos and universities. Consumers who posted their pictures to a specific website like Facebook did not consent or even anticipate the secret “scraping” of those photos by Clearview. Nor could consumers anticipate the subsequent commercialization of their photos by Clearview for secret and unrestricted private searches. Courts should not adopt a rule that would require consumers never to post photos online in order to maintain

basic levels of privacy. *See Jones*, 565 U.S. at 418 (“secrecy” should not be a “prerequisite for privacy.”).

Up until now, one “simply could not” secretly match photos of another person walking down a street in order to identify who that person is. *Jones*, 565 U.S. at 430. Clearview’s app now does that. This “powerful new tool” resulting from “the progress of science” carries enormous encroachment into our privacy. *Carpenter*, 138 S. Ct. at 2223. The Supreme Court has dictated that where technology carries the “features of human anatomy” (like GPS devices and cell phones that track our movements), expectations of privacy must be upheld. *Id.* at 2228.

Here, the precise facial recognition matching technology used by Clearview creates a new ability for users of the app to exploit our basic anatomy (an image of one’s face) to facilitate unrestricted searches and identification. Clearview has effectively mapped who we are and sold it to countless third parties (and even other countries) with an encouragement to “run wild” with this technology. *Van Tassel Ex. 8*. Indeed, Clearview’s app is exactly the kind of “sense-enhancing” technology that the Supreme Court has found to be unlawful. *See Kyllo v. United States*, 533 U.S. 27, 33 (2001) (law enforcement’s use of thermal imaging technology to obtain information from the inside of a home constituted a search, and noting that the Fourth Amendment doctrine “must take account of more sophisticated systems that are already in use or in development”).

In sum, any reasonable person would be highly offended by Clearview’s conduct, because no reasonable person could have anticipated the surveillance use

of the sophisticated and powerful searching and matching capability of Clearview's app. *See State v. Koenig*, 2016 VT 65, ¶ 14, 202 Vt. 243, 249, 148 A.3d 977, 982 (2016) (Vermont Article 11 protection hinges on "public norms" and expectations of privacy are those "that society is prepared to recognize as reasonable."). Therefore, the privacy implications of Clearview's app are readily apparent and immediate, and thus warrant judicial intervention now.

B. Defendant's conduct is unfair because it violates contracts and website terms of service.

Defendant violated the contracts and terms of service of the websites it scraped (Count I). Clearview acknowledges that it went on countless websites like Google, Facebook and Twitter and scraped those websites' photos without authorization. This violated those websites' contracts and terms of service. *Van Tassel Ex. 3* (noting that Google and Facebook sent cease-and-desist letters to Clearview for violations). Further, to the extent Clearview scraped a Vermont business website, this too is a CPA violation.

Clearview did not obtain *any* consent, either from those websites or from the consumers themselves, to use their photos. One of the "founding principles of privacy" is that "personal data should not be used outside of the stated purposes of the [data system] as reasonably understood by the individual, unless the informed consent of the individual has been explicitly obtained." *Supra* note 8, *The Perpetual Line-up Report* at 20 (quotation omitted).

Clearview's failure to obtain any permissions for its photo scraping is an unfair act, because Clearview violated the clear contractual terms of service of

those websites. *See, e.g., Cappello v. Walmart Inc.*, 394 F. Supp. 3d 1015, 1024 (N.D. Cal. 2019) (allowing consumer protection claim for unfairness where Walmart disclosed customers' purchases to Facebook without customer consent in violation of privacy policy, and noting the policy of "holding companies accountable to their own privacy policies [and contracts]"); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583 (1st Cir. 2001) (computer scraping program that mined data of travel website was an unauthorized access: "Explorica's wholesale use of EF's travel codes to facilitate gathering EF's prices from its website reeks of use—and, indeed, abuse—of proprietary information that goes beyond any authorized use of EF's website."); *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (holding that a defendant "exceeds authorized access" when violating policies governing authorized use of databases).

Similarly, Clearview greatly exceeded its authorized access when it scraped photos without permission from those websites or the consumers themselves. For example, numerous websites like Facebook, Google, YouTube, LinkedIn, Venmo, and Twitter, all have terms of service that expressly prohibit Clearview's actions. *See supra* "Background and Facts" at 6-7 (noting that "robots," "scraping" and "other automated means" of "collecting or harvesting" any information or data on those websites is "expressly prohibited," "unless permitted by that person" or "you obtain prior permission" from those websites). Social media websites also have technological safeguards to ward off scrapers and robots, Compl. ¶ 39, which Clearview bypassed.

Additionally, to the extent that Vermont businesses had websites that were scraped by Clearview, this too would be a violation of the CPA. A Vermont business is a “consumer” and thus entitled to the same protections that prohibit unfair acts. *Rathe Salvage, Inc. v. R. Brown & Sons, Inc.*, 2008 VT 99, ¶ 21, 184 Vt. 355, 365, 965 A.2d 460, 467 (2008) (“we hold unequivocally that business entities are entitled to the same rights under the Act as other consumers”). Thus, any violations by Clearview of those Vermont business websites and terms of service are enforceable under the CPA.¹²

At a minimum, Clearview “must obtain the other party’s consent before” using consumers’ photos from any websites, such as Facebook or Google. *Douglas v. U.S. Dist. Court for Cent. Dist. of California*, 495 F.3d 1062, 1066 (9th Cir. 2007) (noting that “a party can’t unilaterally change the terms of a contract”). See also *Goldman v. Breitbart News Network, LLC*, 302 F. Supp. 3d 585, 596 (S.D.N.Y. 2018) (finding copyright violation for using an image from another website without permission in part because defendant did not obtain authorization).

An injunction is thus appropriate to remedy Clearview’s conduct that breached consumer consent requirements. *FTC v. Accusearch Inc.*, 570 F.3d 1187, 1203 (10th Cir. 2009) (Upholding FTC injunction against company that disclosed telephone records without consumer consent and terms of service prohibited such disclosure).

¹² This claim would be distinct from any privacy rights those Vermont businesses may have, see *supra* section A.

C. Defendant's conduct is unfair because it fails to protect consumers' data.

Defendant has violated the public policy expressed in data protection laws by not having adequate protections in place to protect sensitive consumer data (Count I). Courts have already found a lack of reasonable security protections to be an unfair act under consumer protection laws. *See, e.g., In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 990 (N.D. Cal. 2016) (in analyzing the unfairness prong of California's consumer protection law, the court noted that California had a "public policy of protecting customer data" and finding that "Defendants' actions [failure to protect customer data] violated this public policy"); *see also FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 249 (3d Cir. 2015)) (upholding judgment against Wyndham hotels for their data breach, noting that Wyndham's failure to have reasonable data security constituted an unfair act under the FTC Act, and "reject[ing] Wyndham's arguments that its conduct cannot be unfair").

Here, Clearview has already had a data breach. On February 26, 2020, it was reported that Clearview's entire customer list was stolen. Van Tassel Ex. 6; Bailey Ex. 1. Clearview also makes false claims that its data is secure (*see infra* section D). However, Clearview has not demonstrated that it has reasonable protections in place to protect consumers' data, and likely does not given its recent breach. Van Tassel Ex. 6; Bailey Ex. 1. Hence, these failures to protect critical data are unfair acts. *See, e.g., FTC v. Equifax Inc.*, Case No. 1:19-mi-99999 (N.D. Ga. July 22, 2019) (FTC settlement to resolve Equifax data breach and finding

that “Defendant has failed to provide reasonable security for the sensitive personal information collected, processed, maintained, or stored within Defendant’s computer networks.”).¹³

D. Defendant’s conduct is deceptive because of several misrepresentations around its privacy protections, data security, and product.

Defendants makes at least three core sets of material misrepresentations regarding its business and its app (Count II). These are deceptive acts under the CPA.

First, Clearview claims that consumers have “data protection rights” and can “opt-out” and remove their images, but this is deceptive and misleading. Van Tassel Ex. 10; Compl. ¶¶ 56-58. For one, consumers are mostly unaware that Clearview even took their images. The mere fact that Clearview secretly scraped the internet to obtain consumers’ photos could be found deceptive. *See, e.g. In re: Epic Media Group, LLC*, Docket No. C-4389 (FTC Mar. 19, 2013) (FTC found that deceptive acts included “history sniffing” where company secretly tracked 54,000 websites that consumers visited for purposes of doing targeted advertising).¹⁴

Moreover, only California has a law that confers the opt-out rights cited by Clearview’s Privacy Policy. No other citizen in the United States would be able to remove their images using the opt-out procedure cited in Clearview’s Privacy

¹³ Available at: <https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related> (last visited Mar. 9, 2020).

¹⁴ Available at: <https://www.ftc.gov/news-events/press-releases/2012/12/ftc-settlement-puts-end-history-sniffing-online-advertising> (last visited Mar. 9, 2020).

Policy. Compl. ¶¶ 57-58. Even if consumers did request removal, Clearview currently has no such technological capability to detect photos based on geography, residence, and more importantly, age. Compl. ¶ 51. Thus, Clearview cannot actually remove minors' photos, and may not be able to remove any individual's photos with reasonable accuracy. Accordingly, Clearview's statement that it "actively work[s]" to remove images of minors from California is also false. Van Tassel Ex. 2.

Second, Clearview misrepresents that its data is secure. Van Tassel Ex. 10. Its data security assurances overstate the level of security it is able to supply and are thus misleading. *See id.* ("We secure all personal information that we store on computer servers in a controlled, secure environment, protected from unauthorized access, use or disclosure."). In the realm of data security, there are high likelihoods of breaches. *See* Compl. ¶¶ 66-67 (In Clearview's own words, "Unfortunately, data breaches are part of life in the 21st century."). This is especially so with respect to databases containing highly sensitive information like facial recognition identifiers. *See supra* note 10, *FTC Facing Facts Report* at 7 ("databases of photos or biometric data may be susceptible to breaches and hacking."). *See also* Justin H. Dion & Nicholas M. Smith, *Consumer Protection: Exploring Private Causes of Action for Victims of Data Breaches*, 41 W. New Eng. L. Rev. 253, 282 (2019) (surveying wide susceptibility of data breaches in emerging technologies).

And in fact, Clearview just had its first data breach—or at least the first breach that is publicly recognized. As of February 26, 2020, Clearview acknowledged that “an intruder ‘gained unauthorized access’ to its customer list which includes police forces, law enforcement agencies and banks.” Van Tassel Ex. 6; Bailey Ex. 1.

In short, Clearview cannot make the kind of absolute, unqualified guarantees of security that it has, especially in light of its most recent data breach. This is deceptive conduct and is exactly the situation where “an ordinary consumer would need [the] omitted information to evaluate the product or service,” i.e., whether the data is secure. *Carter*, 168 Vt. at 56. *See also In re: Cambridge Analytica, LLC*, Docket No. 9383 (FTC Nov. 25, 2019) (FTC settlement where company made misrepresentations about its privacy certifications).¹⁵

Third and lastly, Clearview makes a number of generally false statements regarding its product and business model. Clearview claims that its product is only used by law enforcement, but that was proven false by the data breach. That breach revealed Clearview’s lengthy customer list of private and large businesses like Verizon, Kohl’s, Rite Aid, Home Depot, the NBA, as well as many universities, and foreign countries like the United Arab Emirates and Saudi Arabi, among countless other who were granted access to Clearview’s app. Van Tassel Ex. 7. *See also Van Tassel Ex. 9* (for over a year, Clearview’s app had been

¹⁵ Available at: <https://www.ftc.gov/enforcement/cases-proceedings/182-3107/cambridge-analytica-llc-matter> (last visited Mar. 9, 2020).

given to wealthy friends, clients and investors for “fun”). Clearview also claims that its product was used to solve crimes in New York City, which the NYPD explicitly refuted. Compl. ¶¶ 74-75. Clearview claims that its facial matching accuracy is 98-99%, but this does not comport with the accepted protocols for facial recognition accuracy. Compl. ¶¶ 71-73. Further, the Georgetown Law Center on Privacy & Technology explains that “[f]ace recognition is less accurate than fingerprinting, particularly when used in real-time or on large databases.” *Supra* note 8, *The Perpetual Line-up Report* at 3. Clearview’s app is both real-time and a large database of unverified photos. Thus, it has enormous capacity to return false results and be highly inaccurate. Lastly, facial recognition technology is generally more inaccurate for persons of color. *See id.* (“Police face recognition will disproportionately affect African Americans” and noting several studies that found that “face recognition may be less accurate on black people.”). *See also* Compl. ¶ 19 (facial recognition was 10 to 100 times inaccurate for African Americans or Asians).

In sum, all of the above-described statements and omissions are misleading. “The capacity to mislead is the prime ingredient of all types of consumer fraud.” *Cox v. Sears Roebuck & Co.*, 138 N.J. 2, 17, 647 A.2d 454, 462 (1994). Thus, Defendant has committed deceptive acts under the CPA.

E. Defendant’s conduct is unfair because it is immoral, unethical and oppressive.

The sum total of Defendant’s conduct of secretly harvesting nearly every available facial photo on the internet, including children, and facilitating search

and identification by third parties (such as law enforcement, businesses, banks, private organizations, universities, celebrities, and even foreign countries), amounts to conduct that is “immoral, unethical, oppressive, or unscrupulous.”

Christie, 136 Vt. at 601. Specifically:

- Clearview scraped the internet, gathering three billion photos, in violation of the contractual terms of service for every website that Clearview scraped;
- Clearview copied and took possession of three billion images without any consent from those consumers who own their images;
- Clearview knowingly acquired photos of children;
- Clearview acquired its data in violation of Vermont’s express data collection law (*see infra* section F);
- Clearview applied biometric AI to consumers in its database for purposes of unrestricted searching and identification;
- Clearview then commercialized all of this into a surveillance product sold to countless entities, including major businesses and organizations, foreign countries, and law enforcement, among others;
- Clearview encouraged users of its technology to engage in unrestricted and “wild” searches;
- Clearview does not have enforceable protocols to prevent against misuse and abuse, and, in fact, acknowledges that unauthorized users have accessed its app;

- Despite possessing consumers' highly sensitive biometric information, Clearview does not have adequate data security measures to prevent breaches and the consequent untold harms that could result (such as fraud, identity theft and even espionage); and
- Clearview misrepresented critical aspects of its business and product (*see supra* section D).

Thus, the State will prevail on all counts of the Complaint (Counts I-III) because all of this conduct amounts to immoral, unethical, oppressive or unscrupulous behavior, which constitutes an unfair act. *See Christie*, 136 Vt. at 601 (unfair acts are those that are immoral, unethical, oppressive or unscrupulous).

Numerous instances of far-reaching technology have risen to immoral and oppressive levels under less egregious circumstances, particularly when they involve lack of consent and/or inability to remove or stop the conduct. *See, e.g., Gantchev v. Predicto Mobile, LLC*, No. 09 C 2312, 2009 WL 3055317, at *3 (N.D. Ill. Sept. 18, 2009) (noting that “conduct is unethical or oppressive if it deprives plaintiffs of a meaningful choice or imposes an unreasonable burden on them” and finding that unauthorized telephone charges were unfair acts); *Centerline Equip. Corp. v. Banner Pers. Serv., Inc.*, 545 F. Supp. 2d 768, 780 (N.D. Ill. 2008) (unsolicited faxes are unfair and oppressive acts: “Conduct is oppressive only if it imposes a lack of meaningful choice or an unreasonable burden on its target. A practice of sending unsolicited faxes does deprive consumers of choice, given that

they cannot avoid such faxes without turning off their fax machines.”); *Henderson v. United Student Aid Funds, Inc.*, 918 F.3d 1068, 1076 (9th Cir. 2019) (unsolicited automated messages from debt collectors violate consumer protection act); *Votto v. Am. Car Rental, Inc.*, 273 Conn. 478, 485, 871 A.2d 981, 985 (2005) (Car rental agency that increased a repair charge without customer’s consent was “without question unscrupulous, immoral and oppressive” under the unfairness prong of Connecticut consumer protection statute).

Similarly, consumers gave no consent to Clearview to use and disseminate their photos. Indeed, most people probably are unaware that they are now in a searchable database of photos for unrestricted use by anyone who bought or obtained Clearview’s app (including businesses like Verizon, Macy’s and Walmart, etc.). Further, consumers have no ability to remove their photos at this time.

While Clearview states that it will process “opt-out requests,” this appears to be false. For one, a close reading of Clearview’s Privacy Policy wherein it expresses the “right to delete” includes an opaquely-worded reservation clause in which it states that it will only honor a deletion request in jurisdictions where there is a regulation requiring them to do so. *Van Tassel Ex. 10*. No such specific regulation exists in Vermont, or in the vast majority of the United States. Compl. ¶¶ 57-58.

Clearview’s app goes far beyond any reasonable consumer’s expectation of how their photos may be used once they are uploaded to a particular website. When a consumer posts a photo to Facebook or Google, they have no ability to

predict that Clearview would copy it, commercialize it, and more importantly assign a biometric identifier to that photo *as a person*. This is not merely a reproduction of a photo. *See e.g., Goldman v. Breitbart News Network, LLC*, 302 F. Supp. 3d 585, 596 (S.D.N.Y. 2018) (distinguishing Google as a “mere indexer” of “the web so that users can more readily find the information they seek” versus a website that intentionally and unlawfully posted a user’s photo without permission: “Google’s search engine provided a service whereby the user navigated from webpage to webpage, with Google’s assistance. This is manifestly *not* the same as opening up a favorite blog or website to find a full color image awaiting the user, *whether he or she asked for it*, looked for it, clicked on it, or not.”) (emphasis added).

Clearview’s app thus constitutes oppressive and unscrupulous conduct by taking private photos through unauthorized scraping of various social media platforms to create a surveillance program in violation of substantial privacy interests, among other interests like data security (*see supra* section C). Further, Clearview’s misstatements about its product, privacy, and data security are also unscrupulous (*see supra* section E).

In sum, *all* of Clearview’ conduct (*see generally* Complaint) rises far above the typical unauthorized acts involved in other oppressive technology cases like unsolicited faxes, automated messages, etc. *See supra* cases cited above. Therefore, it must be enjoined as immoral, unethical, oppressive and/or unscrupulous.

F. Defendant's conduct violates Vermont's Fraudulent Acquisition of Data Law.

Defendant has violated Vermont's data acquisition law, 9 V.S.A. § 2431 (Count III).

This law (effective January 1, 2019) arose out of the Legislature's concern that information acquired by data brokers could be used in order to facilitate illegal acts. 2018 Vt. Acts & Resolves No. 171, § 1(a)(3).¹⁶ The Legislature also deemed it important to protect consumers' data and prevent misuse and abuse of their data. *Id.* at § 1(a)(1)(D), (G).

The data broker law is enforceable under the CPA. "A person who violates a provision of this section commits an unfair and deceptive act in commerce in violation of section 2453 of this title." 9 V.S.A. § 2431(b).

In this matter, Clearview violated the prohibition in the data acquisition law that prohibits fraudulent acquisition of data. 9 V.S.A. § 2431(a)(1) (prohibiting "acquisition of 'brokered personal information' through fraudulent means"). Clearview acquired its data (consumers' photos) through "screen scraping," the practice of collecting information from a website via an automated process. Screen scraping is improper because it violates the purpose and the spirit of a website interaction. For example: if I upload a photo to a social media site like Facebook or Twitter, it is so that I can share it with other Facebook or Twitter users, as guided by the express terms and conditions of those sites, including their

¹⁶ Available at:

<https://legislature.vermont.gov/Documents/2018/Docs/ACTS/ACT171/ACT171%20As%20Enacted.pdf> (last visited Mar. 9, 2020).

privacy settings. Other people who want to look at my photo must interact with the website in the manner and under the rules established by the platform. When I join the website, I agree to abide by its terms of service, and I rely on the website's compliance with its promises and obligations, particularly that the photo will remain on the website under the promised conditions. The data that we post is valuable, and unfortunately it is possible to use technology to steal that data for uses that were not intended by either the consumer or the website.

Interaction with a website is premised on agreeing to comply with its terms of service. Compl. ¶¶ 42-43. Many of the websites from which Clearview collected its data had explicit prohibitions against the use of screen scraping. *Id.* Those websites also tried to prohibit Clearview's scraping practice through the use of anti-scraping technology. Clearview interacted with numerous websites (including YouTube, Facebook, LinkedIn and Twitter) using automated processes to steal the data on those websites. That data was uploaded by consumers in reliance on those websites' terms of service. Clearview's automated scraping of the data was thus in direct violation of the agreements that Clearview was required to enter into in order to use the websites. *See supra* "Background and Facts" at 6-7.

Therefore, Clearview's behavior constitutes fraudulent acquisition of data under 9 V.S.A. § 2431(a)(1).

Request for Relief

Courts have the authority to restrict activities in order to eliminate unfair or deceptive practices. *See FTC v. National Lead*, 352 U.S. 419, 510 (1959) (upholding

FTC's restriction of lawful activities in order to prevent a continuance of unfair competitive practices). Here, a preliminary injunction is warranted to restrict Clearview's unfair and deceptive acts and practices.

There is particular urgency in this matter. For one, Clearview is a new technology company, and its reach appears to be far beyond that of any other facial recognition company that exists today. *Supra* note 10, *FTC Facing Facts Report* at 8 (even the FTC did not know of companies doing what Clearview does); *supra* note 8, *The Perpetual Line-up Report* at 20 (in discussing law enforcement's own database of facial recognition images such as mug shots, drivers' licenses, and unsolved photo files, the Report noted that "[n]ever before has federal law enforcement built a biometric network primarily made of law-abiding Americans."). A preliminary injunction is needed before Clearview becomes an entrenched market participant and the genie is effectively out of the bottle. An injunction will also ensure appropriate safeguards are in place before this technology becomes further embedded in nationwide government and commercial uses. There is also no limit on who Clearview may choose to sell to next. *See, e.g., Van Tassel Exs. 7, 9 and 11.*

Next, the risk to Vermonters' data security is an immediate harm. Clearview has already suffered a data breach. Databases of photos and biometric data are particularly sensitive information. *Patel*, 932 F.3d at 1269 ("if compromised by hackers, biometric data are biologically unique to the individual, and once compromised, the individual has no recourse [and] is at heightened risk for identity theft."). This sensitive trove of consumer biometric information is also particularly

“susceptible to breaches and hacking.” *Supra* note 10, *FTC Facing Facts Report* at 7.

A preliminary injunction is necessary now to ensure the appropriate data security protections are in place *before* Clearview’s product is deployed *en masse* even further and subsequently breached further.

Lastly, a preliminary injunction is needed because of the heightened risk of misuse of Clearview’s app. *See, e.g., supra* note 8, *The Perpetual Line-up Report* at 2 & 4 (noting that many facial recognition systems are “out of control” and that most “[m]ajor face recognition systems are not audited for misuse.”). Clearview’s app has been used by unauthorized persons. Compl. ¶ 32. The potential for misuse is even greater because of the inclusion of children in the database. Vermonters, and their children, should not have to continue to suffer significant ongoing privacy violations before this Court can act.

Conclusion

For the foregoing reasons, the State respectfully requests that the Court issue an order requiring that Defendant:

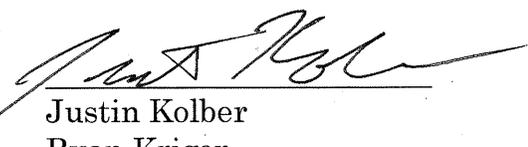
1. Cease collecting all photos of Vermonters, including Vermont children;
and
2. Delete or destroy all photos and facial recognition identifiers of Vermonters from its app and/or database, including Vermont children.

DATED at Montpelier, Vermont, this 10th day of March 2020.

Respectfully submitted,

STATE OF VERMONT

THOMAS J. DONOVAN, JR.
ATTORNEY GENERAL

By: 

Justin Kolber

Ryan Kriger

Jill Abrams

Assistant Attorneys General

Office of the Attorney General

109 State Street

Montpelier, VT 05609-1001

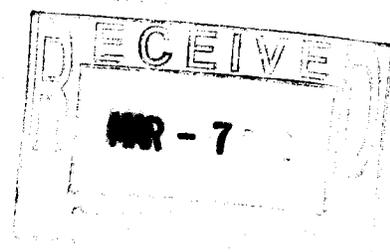
(802) 828-3171

justin.kolber@vermont.gov

ryan.kriger@vermont.gov

jill.abrams@vermont.gov

STATE OF VERMONT



SUPERIOR COURT
Washington Unit

CIVIL DIVISION
Docket No. 484-7-10 Wncv

STATE OF VERMONT,)
Plaintiff)
)
v.)
)
CSA-CREDIT SOLUTIONS)
OF AMERICA, LLC and)
DOUG VAN ARSDALE,)
Defendants)

2012 MAR - 5 P 3:29
 AS
 VERMONT SUPERIOR COURT

DECISION AND ORDER: MOTION FOR SUMMARY JUDGMENT

I. INTRODUCTION

The State of Vermont, by the Office of the Attorney General, filed this lawsuit under the Consumer Fraud Act, 9 V.S.A. chapter 63, in which it alleged four categories of consumer fraud violation by CSA-Credit Solutions of America (“CSA”), a Texas-based “debt settlement” company, and by Doug Van Arsdale, its chief executive. The suit alleges that Defendants (a) used deceptive and unsubstantiated online “results” claims to advertise their services to economically distressed consumers, (b) failed to comply with statutory requirements relating to consumers’ right to cancel their contract with CSA, (c) failed to abide by many provisions of the Vermont Debt Adjusters Act, and (d) employed an advance-fee structure that constituted an unfair trade practice. The first three of these causes of action are the subject of a Motion for Summary Judgment filed by the State.

This action was filed on July 2, 2010; Defendants’ Answer was filed on July 9, 2010. On September 20, 2011, Defendants’ counsel moved for leave to withdraw. On September 29,

the motion was granted and Defendants were directed to have successor counsel file a notice of appearance within 45 days. To date, the Court has received neither notice of appearance by counsel nor a notice of self-representation. On November 18, Plaintiff filed its Motion for Summary Judgment with supporting documents.¹ To date, Defendants have not responded to the motion in any manner.

II. THE STANDARDS GOVERNING SUMMARY JUDGMENT

The procedure for summary judgment is authorized by Rule 56 of the Vermont Rules of Civil Procedure. That rule provides a method by which a case, or a claim or defense, may be disposed of before trial where no genuine issue as to any material fact exists, or where only a question of law is involved. As stated in Rule 56(c), “[t]he judgment sought shall be rendered forthwith if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that the moving party is entitled to a judgment as a matter of law.”

The moving party has the burden of establishing that there exist no issues of material fact, and that the movant is entitled to judgment as a matter of law. *Gore v. Green Mountain Lakes, Inc.*, 140 Vt. 262, 264 (1981). On the other hand, where the issue before the court is solely one of law, and the moving party is entitled to judgment as a matter of law, the granting of summary judgment is appropriate. *Garneau v. Curtis & Bedell, Inc.*, 158 Vt. 363, 366 (1992). Moreover, opposing allegations must have sufficient support in specific facts to create a genuine issue of material fact, *Baldwin v. Upper Valley Services, Inc.*, 162 Vt. 51, 55 (1994); mere denial of the moving party’s pleadings is not enough. *Gendreau v. Gorczyk*, 161 Vt. 595, 596 (1993) (mem.). All material facts set forth in the statement

¹ The motion was anticipated by an amended Discovery Stipulation and Order filed by the parties on September 29, 2011.

required to be served by the moving party will be deemed to be admitted unless controverted by the statement required to be served by the opposing party. V.R.C.P. 56(c)(2).

III. THE MATERIAL FACTS AS TO WHICH THERE IS NO GENUINE ISSUE TO BE TRIED

As required by V.R.C.P. 56(c)(2), the State annexed to this Motion a Statement of Material Facts as to Which There is No Genuine Issue to Be Tried.). Since the Defendants have not controverted any of the statements submitted by the Plaintiff, the Court deems them to be admitted. *Gallipo v. City of Rutland*, 2005 VT 83, ¶ 33, 178 Vt. 244. Material facts from the Statement are referred to below as “MF” followed by their corresponding number, as in “MF 13.”

IV. OVERVIEW OF DEFENDANTS’ BUSINESS AND INDUSTRY

Defendant CSA-Credit Solutions of America, LLC, is a Delaware limited liability corporation with offices in Dallas, Texas. MF 1. The company is engaged in the business of settling consumer debts with the creditors to whom the debts are owed. MF 2. CSA-Credit Solutions of America, LLC, is the surviving entity of a December 2009 merger with CSA-Credit Solutions of America, Inc. MF 3. The former has stipulated that it is liable for the actions of its “Inc.” predecessor.² MF 4.

Defendant Doug Van Arsdale is a resident of Texas. MF 5. In December 2003, he founded CSA (Inc.). MF 6. He then served as Chief Executive Officer and Director of the company until November 2006 and Registered Agent until June 2007. MF 7. In December 2007, Mr. Van Arsdale resumed his positions as Chief Executive Officer and Registered Agent of the corporation. MF 8. He was also the sole owner of CSA from December 2003 to

² In the remainder of this , CSA-Credit Solutions of America, Inc., and CSA-Credit Solutions of America, LLC, are referred to as “CSA.”

November 2006, and from December 2007 until December 2009. MF 9. In December 2009, he founded CSA (LLC), of which he has served as Manager and Governing Person. MF 10.

At all times relevant to this action, CSA held itself out as a “debt settlement” company offering to negotiate reductions in the principal amount of consumers’ debts. MF 11. CSA advertised its services through its Internet website, and consumers who wished to respond either called CSA or provided their contact information on the website and received a return call from CSA.³ MF 12.

Under CSA’s Terms of Agreement—also called its Client Service Agreement, MF 14—consumers “enrolled” their debts with CSA in exchange for service fees. MF 15. CSA was responsible for negotiating settlement offers on those debts. MF 16. Consumers were to make contractually-specified monthly payments into a bank account, out of which CSA’s fees were electronically drawn by the company. MF 17. Consumers were responsible for depositing additional monies to pay any agreed-upon settlements to their creditors. MF 18.

CSA’s service fees were typically calculated as 15 percent of the principal amount of each debt enrolled in its program, MF 19, and paid during the first months of enrollment. MF 20. For example, one Vermont consumer with \$42,400 in debts was charged fees of 15 percent of that amount, or \$6,360, of which \$636 was paid in each of the first four months, and \$318 was paid in each of the next 12 months; the consumer was also expected to set aside an additional \$332 a month for 12 months to fund debt settlements. MF 21.

At its height, CSA had 1,200 employees, including some 400 sales staff. MF 22. The company’s website referred at various times to having enrolled 250,000 consumers, MF 23, with enrolled debts worth a total of more than \$1 billion. MF 24.

³ CSA may also have called some other consumers whose names were provided by “lead generators.” MF13.

CSA is a member of an industry described by the FTC as offering debt settlement plans that, “as they are often marketed and implemented, raise[d] several consumer protection concerns.” One concern of direct relevance to the instant motion is advertising that made what the FTC termed “false, misleading, or unsubstantiated representations,” such as claims that “the provider will or is highly likely to obtain large debt reductions for enrollees, *e.g.*, a 50% reduction of what the consumer owes,” and that “the provider will or is highly likely to eliminate the consumer’s debt entirely in a specific time frame, *e.g.*, 12 to 36 months.” FTC, Telemarketing Sales Rule, Final Rule Amendments, 75 Fed. Reg. 48458, 48463 (Aug. 10, 2010) (hereinafter “*FTC*”).

Between January 19, 2004, and October 29, 2008,⁴ 207 Vermonters paid CSA over \$350,000 in debt settlement fees, net of refunds.⁵ MF 26.

V. STATUTORY FRAMEWORK: THE VERMONT CONSUMER FRAUD ACT—DECEPTION, UNFAIRNESS, AND LACK OF SUBSTANTIATION

A. Introduction

The legal framework for most of the State’s causes of action in this case is provided by the Vermont Consumer Fraud Act.⁶ That statute prohibits any unfair or deceptive act or practice in commerce. *See* 9 V.S.A. § 2453(a). In applying the concepts of unfairness and deception, the courts of Vermont are to be “guided” by precedent from the FTC and the federal courts. 9 V.S.A. § 2453(b).

The Consumer Fraud Act is a remedial statute, to be interpreted liberally to effectuate its purpose of protecting consumers. *See, e.g., Carter v. Gugliuzzi*, 168 Vt. 48, 52

⁴ Of the 207 Vermont consumers enrolled with CSA, all but 3 signed up before the start of 2008, and all but 66 before the start of 2007. MF 25.

⁵ According to CSA’s data, Vermonters paid a total of \$371,886.43 and received refunds of \$18,051.06, for a net of \$353,835.37. MF 27.

(1998) (“The express statutory purpose of the Act is to ‘protect the public’ against ‘unfair or deceptive acts or practices.’ ... Its purpose is remedial, and as such we apply the Act liberally to accomplish its purposes.”); *Sawyer v. Robson*, 181 Vt. 216, 223 (2006) (“As we emphasized in *Elkins [v. Microsoft]*, 174 Vt. 328, 331 (2002), ‘The Legislature clearly intended the [Consumer Fraud Act] to have as broad a reach as possible in order to best protect consumers against unfair trade practices.’”); *State v. Custom Pools*, 150 Vt. 533, 536 (1988) (“[T]he Act is clearly remedial in nature. Therefore, we must construe the statute liberally so as to furnish all the remedy and accomplish all the purposes intended.”); *accord*, *State v. Therrien*, 161 Vt. 26, 30-32 (1993), and *Fancher v. Benson*, 154 Vt. 586 (1990).

B. The Consumer Fraud Act Prohibits Deceptive Trade Practices.

The Consumer Fraud Act prohibits deceptive acts and practices in commerce. 9 V.S.A.

§ 2453(a). As noted in *Carter v. Gugliuzzi*, 168 Vt. at 56, deception has three elements:

(1) there must be a representation, omission, or practice likely to mislead consumers; (2) the consumer must be interpreting the message reasonably under the circumstances; and (3) the misleading effects must be material, that is, likely to affect the consumer’s conduct or decision regarding the product. ... Deception is measured by an objective standard, looking to whether the representation or omission had the “capacity or tendency to deceive” a reasonable consumer; actual injury need not be shown. ... To be reasonable, moreover, the consumer’s understanding need not be the *only* one possible; “[i]f an ad conveys more than one meaning to reasonable consumers and one of those meanings is false, that ad may be condemned.” ... Furthermore, the Act “does not require a showing of intent to mislead, but only an intent to publish the statement challenged.” [Citations omitted.]

The third element of deception, materiality, is measured by an objective standard, based on what a reasonable person would regard as important in making a decision. *Carter*, 168 Vt. at 56 (citing *In re Cliffdale Assocs.*, 103 F.T.C. 110, 179 (1984)). The federal courts and the FTC apply a general presumption of materiality: “Where the seller knew, or should

⁶ The other statute relied upon in this lawsuit is the Vermont Debt Adjusters Act.

have known, that an ordinary consumer would need omitted information to evaluate the product or service, or that the claim was false, materiality will be presumed because the manufacturer intended the information or omission to have an effect.” *Id.* at 56 (quoting *Cliffdale*, 103 F.T.C. at 182). Express claims are automatically deemed to be material. *Id.*

C. The Consumer Fraud Act Prohibits Unfair Trade Practices.

In addition to prohibiting deceptive trade acts and practices, the Consumer Fraud Act, 9 V.S.A. § 2453(a), bans unfair acts and practices in commerce. The definition of unfairness is set out in *Christie v. Dalmig*, 136 Vt. 597, 601 (1979) (quoting *F.T.C. v. Sperry & Hutchinson Co.*, 405 U.S. 233, 244 n.5 (1972)):

“(1) whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise—whether, in other words, it is within at least the penumbra of some common-law, statutory, or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive or unscrupulous; [or] (3) whether it causes substantial injury to consumers...”

While the FTC has stated that substantial injury is the most important of the three alternative formulations of unfairness, it has also noted that violation of public policy as established by statute (among other legal sources) can be used either to support an unfairness claim based on substantial consumer injury or to demonstrate on its own that such injury is present, as long as the public policy is “clear and well-established.” Commission Statement of policy on the Scope of the Consumer Unfairness Doctrine, Appendix to *In re International Harvester*, 104 F.T.C. 949, 1984 WL 565290 at *95, *98-99.⁷

D. Lack of Prior Reasonable Substantiation Is Both Deceptive and Unfair.

⁷ In *Lalande Air & Water Corp. v. Pratt*, 173 Vt. 602 (2002), the Vermont Supreme Court also analyzed unfairness in terms of its oppressive or unscrupulous character under that alternative prong of the *Sperry & Hutchinson* standards, although there it did not find the acts at issue—sending demand letters and filing suit to collect rent beyond that allowed by a ruling whose constitutionality was under legal challenge—to be unfair.

A key requirement of commercial advertising is that the advertiser must possess prior reasonable substantiation for any factual claims that are made. *See* Policy Statement Regarding Advertising Substantiation Program, 49 Fed. Reg. 30999 (Aug. 2, 1984) (“We affirm our commitment to the underlying legal requirement of advertising substantiation—that advertisers and ad agencies have a reasonable basis for advertising claims before they are disseminated.”) It has been held to be *both* unfair and deceptive for a person to make factual claims to prospective customers without prior reasonable substantiation.

For example, analyzing the need for substantiation from the standpoint of unfairness, the FTC stated in *In re Pfizer, Inc.*, 81 F.T.C. 23, 1972 WL 127465 at *29,

[T]he Commission is of the view that it is an unfair practice in violation of the Federal Trade Commission Act to make an affirmative product claim without a reasonable basis for making that claim. Fairness to the consumer, as well as fairness to competitors, dictates this conclusion. Absent a reasonable basis for a vendor’s affirmative product claims, a consumer’s ability to make an economically rational product choice, and a competitor’s ability to compete on the basis of price, quality, service or convenience, are materially impaired and impeded.

At the same time, the FTC has also held a failure to substantiate to be deceptive:

Advertising that lacks a reasonable basis is also deceptive. . . . The deception theory is based on the fact that most ads making objective claims imply, and many expressly state, that an advertiser has certain specific grounds for the claims. If the advertiser does not, the consumer is acting under a false impression. The consumer might have perceived the advertising differently had he or she known the advertiser had no basis for the claim.

Cliffdale Associates, Inc., 103 F.T.C. 110, 1984 WL 565319 at *45 n.5.

Finally, where claims are involved “whose truth or falsity would be difficult or impossible for consumers to evaluate by themselves”—as is true in this case—a “high level of substantiation” is required. *Thompson Medical Co., Inc.*, 104 F.T.C. 648, 1984 WL 565377 at *72.

VI. DEFENDANTS VIOLATED THE CONSUMER FRAUD ACT BY MAKING DECEPTIVE AND UNSUBSTANTIATED RESULTS CLAIMS.

The first of the State's causes of action is that Defendants violated the Vermont Consumer Fraud Act by repeatedly advertising, deceptively and without substantiation, that they could achieve specified results for consumers in terms of settling debts at amounts substantially below the principal balance due. These claims—which were expressed in terms of percentages (e.g., “Settle Debts For 40%-60% Off Balance”) or time (e.g., “Become Debt Free In Less Than 36 Months”)—appeared on CSA's website, through which consumers in financial difficulty were lured to contact the company.

A. CSA Repeatedly Promised Consumers Major Reductions in Their Debts.

CSA solicited potential customers through its Internet website. MF 12. Using that medium, the company advertised its debt settlement services with a succession of prominent, home-page claims about the results that consumers could expect from its services, including:

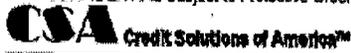
- “Affordable Monthly Payments Settle Debts For 40%-60% Off Balance” (on CSA's website from December 2004 to December 2006).
- “It [debt settlement] specifically reduces your current outstanding total balances 40-60%” (December 2004 to May 2007).
- “Reduce your debt 60% in seconds!” (March 2005 to February 2006).
- “Reduce your debt 50-75% in seconds!” (August 2004 to December 2004).
- “When you hire us, we negotiate with your creditors to settle your outstanding balance by eliminating 40-60% of your debt” (August 2005 to December 2006).
- “Reduce Total Balances 40-60%” (July 2005 to April 2007).
- “Become Debt Free In Less Than 36 Months” (December 2004 to May 2007).
- “Most of our clients become debt free within 36 months or less” (September 2007 to November 2007).
- “A typical settlement can be accomplished within 36 months or less” (December 2004 to May 2007).

- “We help you become debt free in 12 to 36 months” (June 2007 to October 2007). MF 30.

These claims were made continuously through at least 347 modifications of CSA’s website during the years 2004 through 2007, while the company was offering and selling its debt collection services to Vermonters. MF 31.

Moreover, the CSA Enrollment Summary Page (the title was later dropped, but the content remained the same), which was part of the Customer Enrollment Package that CSA mailed to all its customers, MF 32, routinely used a 60% figure to calculate projected savings. MF 33. An example of a Vermont consumer’s Enrollment Summary Page appears below, with a total debt of \$42,400 and an “Estimated Settlement Amount (Approx. 40%)” of \$16,960—which reflects a 60% savings off the amount due at enrollment. MF 34. In his deposition in a lawsuit similar to this one brought by the New York Attorney General, Defendant Van Arsdale agreed that the reference to an estimated 60% savings on this form “would mean that this consumer can anticipate or would reasonably anticipate that they were going to have a savings off of their debt of 60 percent.” *People ex rel. Cuomo v. CSA-Credit Solutions of America, Inc.* (N.Y. Sup. Ct. No. 401225/09) (Deposition of Douglas Van Arsdale, May 25, 2011) (hereinafter “*DVA*”) at 237.⁸ MF 35.

⁸ See also *DVA* at 72 (Q. “CSA was saying to a reasonable consumer you can expect to save 50 percent of your debt [when the CSA website advertised a “50%” savings]?” A. “Sure.”), and *DVA* at 222 (to same effect). MF 36.



Enrollment Summary Page

**** Please Note:** This page must be returned with your Enrollment Package in order for the set up of your file to be completed.

CSA™ Estimated Settlement Plan Cost		CSA™ Service Fee Payment Schedule		Estimated Personal Savings Plan for Payments to Creditors	
Total Unsecured Debt:	42400.00	CSA™ Total Service Fee:	6360.00	Estimated Settlement Amount (Approx. 40%):	16960.00
Estimated Settlement Amount (Approx. 40%):	16960.00	CSA Initial Deposit:	2544.00	Savings Budget During Initial Deposit Payments:	* Optional *
CSA™ Service Fee:	6360.00	4 Initial Deposit Payments of:	636.00	Minimum Savings During 12 Remaining Service Fee Payments:	332.00
Total Debt Elimination Cost:	23320.00	Remaining Service Fee Balance:	3816.00	Minimum Personal Saving Payments After CSA™ Fee is Paid:	650.00
Total Debt Savings:	19080.00	12 Monthly Service Fee Payments of:	318.00	Total Payments towards Savings After All Payments:	17634.00
Estimated Monthly Budget Payments:	650.00	Total Months to Payoff Service Fee:	18	Estimated DEBT FREE Time Frame:	36 Months

**** NOTE:** The estimated saving plan is the minimum suggested for payoff of your enrolled accounts. CSA™ highly recommends that any additional funds, which may become available, be allocated towards your personal savings account. You are encouraged to add as much towards savings as possible, as it is to your advantage to do so. The quicker you save money, the sooner you can get your enrolled debts resolved.

ACH Debt Service Fee Summary / Personal Savings Summary			
Program Start Date:	February 15, 2004	4 Initial Deposit Payments of:	636.00
Remaining Service Fee Start Date:	June 15, 2004	12 Monthly Service Fee Payments of:	318.00
Personal Savings Start Date:	June 15, 2004	12 Personal Savings Deposits of:	332.00
Client Signature:		Date:	

**** Important:** The above debt schedule is the CSA™ recommended payment and personal savings budget. Any date change of your scheduled ACH Debt, CSA™ auto fee accounts, require a minimum of five(5) business days notice.

According to the FTC, “phrases such as ‘as much as’ or ‘up to’ (e.g., ‘up to 60% savings’) likely convey to consumers that the product or service will *consistently* produce results in the range of the stated percentage or amount.” *FTC*, 48500 n. 578 (emphasis added). Thus, while both CSA’s 40% and 60% savings claims must be supported by substantial data, the 40% savings must be *typical*, whereas the 60% savings “only” need be *consistent*. On the other hand, since CSA customarily informed consumers, in its Customer Enrollment Package, that they could expect 60% savings on their debts—and CSA’s principal acknowledges that this was a reasonable expectation—that higher standard should have been met, at a minimum, for most enrolled consumers.

CSA's results claims were not qualified or vague. On the contrary, they were unqualified and quantitative, stating precise percentages, ranges of percentages, or time frames to describe the reduction in principal debt amounts—which is to say, the savings—that consumers could anticipate. On their face, as Defendant Van Arsdale has acknowledged, such claims communicated to reasonable consumers that they could personally expect to achieve the stated results, or, put another way, that those outcomes were typical of what CSA customers would achieve.

B. CSA's Actual Results Were Dramatically Inconsistent with Its Claims.

The Attorney General's Office sought from CSA through discovery in this case all data that would support the company's advertised results claims. MF 37. In response, two sets of data were produced. One set included a spreadsheet containing a list of 903 debts enrolled by Vermont consumers who paid fees to CSA, the dollar amounts of those debts at the time of enrollment, and the dollar amounts of the settlement offers negotiated by CSA, MF 38 (referred to herein as "the Vermont data"). The other data set consisted of a list of 33,390 debts settled between August 2006 and November 2007, the dollar amounts due at the time of settlement (not at the time of enrollment), and the dollar amounts of the settlements (referred to herein as "the national data"), MF 39, from which the percentage savings for each debt for which there was a settlement offer could be computed. (However, as noted *infra* text 18, CSA did not have a "denominator" to compare these results to, and thus could not say whether its national success rate was 50% or 5% or .5%.)

Vermont results. The focus of the State's analysis of the Vermont data was to answer the following questions, in order to determine the accuracy of CSA's advertising of "40%" savings, "60%" savings, and "debt-free":

1. What percentage of Vermont-enrolled debts were the subject of a settlement offer obtained by CSA that met the advertised percentage of 40%, *including* in the calculation the amount of fees the consumer had to pay to CSA?
2. What percentage of Vermont-enrolled debts were the subject of a settlement offer obtained by CSA that met the advertised percentage of 40%, *excluding* from the calculation the amount of fees the consumer had to pay CSA?
3. What percentage of Vermont-enrolled debts were the subject of a settlement offer obtained by CSA that met the advertised percentage of 60%, *including* in the calculation the amount of fees the consumer had to pay to CSA?
4. What percentage of Vermont-enrolled debts were the subject of a settlement offer obtained by CSA that met the advertised percentage of 60%, *excluding* from the calculation the amount of fees the consumer had to pay to CSA?
5. What percentage of Vermont consumers who signed up with CSA were “debt-free” within three years—that is, had a settlement offer negotiated by CSA for all of their enrolled debts?

In 2010, the FTC, relying on existing precedent, provided detailed guidance on how to calculate these numbers. In its commentary on debt settlement amendments to the federal Telemarketing Sales Rule, the agency complained that debt settlement companies “often use [deficiencies in data] to support their savings claims. All of these deficiencies inflate the savings consumers are likely to obtain.” *FTC* at 48499. As a cure, certain principles must be followed:

1. Any savings must be measured against the amount of the debt *at the time of enrollment*.
2. Any savings must take into account the *fees* paid to the debt settlement company.
3. Any savings claims must be based on *all* of the debts enrolled by all of the debt settlement company’s customers, not just on debts that were settled.

As the FTC has stated, “savings claims must be calculated based on the amount of debt owed at the time of enrollment, rather than the amount at the time of settlement, in order to account for (a) increases in debt levels from creditor fees or interest charges that

accrue during the period of the program,^{9]} and (b) fees the consumer pays to the provider. ... [I]n making savings claims, a provider must take into account the experiences of all of its past customers, including those who dropped out or otherwise failed to complete the program. ... In making savings claims, a provider must [also] include all of the debts enrolled by each consumer in the program. The provider may not exclude debts that it has failed to settle—including those associated with consumers who dropped out of the program—from its calculation of the average savings percentage or amount of its consumers' debt reduction.” *FTC* at 48500-49501 (footnotes omitted). Moreover, this guidance from the FTC is based not on some new legal theory, but on the agency’s decades-old legal test for deception.¹⁰

These principles make absolute sense from the viewpoint of a consumer who views an online debt settlement advertisement such as, “Reduce your debt 60% in seconds,” and who, let us say, has a debt on which the balance as of the time of the viewing is \$10,000. Underscoring the importance of calculating savings against the amount of the debt at enrollment (not at settlement), a reasonable consumer should be able to expect a settlement

⁹ The FTC’s description of debts increasing from the date of enrollment to the date of settlement accurately describes what happened to most Vermont consumers. Of 394 debts for which CSA’s data shows both an enrollment amount and a current balance, 358 debts increased from the time of enrollment; the total net increase was \$385,429.72, and the average change in amount was an increase of \$978.25. MF 40.

¹⁰ See *FTC* at 48497 n. 549 (citing FTC’s 1984 Policy Statement on Deception), and *FTC* at 48499 n. 567 (citing FTC cases challenging percentage savings claims that date back to 2002, including *FTC v. Debt-Set*, No. 1:07-cv-00558-RPM (D. Colo. filed Mar. 19, 2007) (promising to reduce amount owed to 50% to 60% of amount at time of enrollment); *FTC v. Connelly*, No. SA CV 06-701 DOC (RNBx) (C.D. Cal. Am. Compl. filed Nov. 27, 2006) (promising to reduce overall amount owed by up to 40% to 60%); *FTC v. Nat’l Consumer Council, Inc.*, No. SACV04-0474 CJC (JWJX) (C.D. Cal. filed Apr. 23, 2004); *FTC v. Better Budget Fin. Servs., Inc.*, No. 04-12326 (WG4) (D. Mass. filed Nov. 2, 2004) (promising to reduce consumers’ debts by up to 50% to 70%); *FTC v. Innovative Sys. Tech., Inc.*, No. CV04-0728 GAF JTLx (C.D. Cal. filed Feb. 3, 2004) (representing it could save consumers up to 70% of debt owed); *FTC v. Jubilee Fin. Servs., Inc.*, No. 02-6468 ABC (Ex) (C.D. Cal. filed Aug. 19, 2002) (promising to reduce debts by up to 60%). Thus, CSA had reason to know that its advertising was deceptive, had it inquired into the matter. Indeed, in another consumer fraud case brought by the State, the Vermont Supreme Court opined that it “must give substantial deference to the FTC’s express position” as articulated not prior to the conduct at issue, but in an *amicus curiae* brief filed in support of the State in that very appeal. See *State v. Internat’l Collection Service, Inc.*, 156 Vt. at 545-46.

offer of 60% off the amount of the debt when she signs up, or \$4,000—not an offer of 60% off some as-yet-unknown higher amount due (higher because of potential future interest, fees, and penalties). Likewise, if the consumer also has to pay \$1,500 in fees, those fees will be real money out of her pocket that reduces her savings and should therefore be taken into account in figuring the actual extent of those savings. Finally, if she were told that the promised 60% reduction in her debt would occur *only if* there is a settlement offer, and that in many cases the company will not be able to obtain such an offer, it is unlikely that she or many other consumers would bother to enroll in the first place.

In response to the State’s discovery requests, CSA produced an Excel spreadsheet that contained key information on the debts enrolled by company’s Vermont customers, including consumer identification information, the amount of the debt at enrollment (“enrollment amount”), and the amount of settlement offers, MF 42; CSA has stipulated that the spreadsheet is the most accurate data compilation for Vermont.¹¹ MF 29. By comparing the debt enrollment amounts to the corresponding best (lowest-dollar) settlement amounts, it is possible to determine how many of the Vermont debts were the subject of a settlement offer that met the terms of CSA’s savings claims (*i.e.*, a 40% or 60% reduction in the amount to be paid to the creditor), and to determine how many Vermonters became “debt-free” (had settlement offers for all of their debts) at any point in time.

Responding to the five questions set out on page 13, above, here are the *actual* results achieved by CSA for Vermonters, based on comparing (1) the dollar amount due at the time of enrollment of the each of the 903 Vermont debts, with (2) the lowest-dollar settlement offer, if any, negotiated by CSA for each of those debts:

¹¹ CSA’s Vermont data actually omitted some settlement offers that the Attorney General’s Office identified from other company documents and added to the spreadsheet, to CSA’s benefit. MF 41.

1. Of the 903 Vermont debts, 63—7.0%—were the subject of an offer in an amount at least 40% less than the enrollment amount of the debt, including CSA’s estimated fees.¹² MF 44.
2. Of the 903 Vermont debts, 139—15.4%—were the subject of an offer in an amount at least 40% less than the enrollment amount of the debt, excluding fees. MF 45.
3. Of the 903 Vermont debts, 6—0.7%—were the subject of an offer in an amount at least 60% less than the enrollment amount of the debt, including CSA’s estimated fees. MF 46.
4. Of the 903 Vermont debts, 44—4.9%—were the subject of an offer in an amount at least 60% less than the enrollment amount of the debt, excluding fees. MF 47.
5. Of the 207 Vermont consumers who signed up with CSA, 31—15.0%—received a settlement offer in any amount for all of their enrolled debts. MF 48.

Restated in tabular form, the first four figures are as follows:

	40% Savings	60% Savings
Counting CSA Fees	7.0%	0.7%
Not Counting CSA Fees	15.4%	4.9%

It is obvious that these Vermont results are not remotely consistent with CSA’s advertised results claims. Indeed, following the FTC framework (and thus including CSA’s fees in the calculation), and focusing on the 60% savings that CSA routinely set out in Vermont consumers’ paperwork, only 0.7% of Vermont consumers’ debts—*one debt in 200*—were the subject of a settlement offer consistent with CSA’s promises. What is more,

¹² CSA’s Vermont data does not link consumer fees paid to the specific debts that form the basis for calculating those fees; the data only shows the total of fees paid by each consumer. To calculate success rates *including fees*, the State multiplied the enrollment amount of each debt by CSA’s customary 15% fee formula; but the fees associated with debts for which there was *no settlement offer* were ignored. This ended up *understating* the total fees that Vermonters paid (and favoring CSA), but it provided the best estimate possible of how much consumers who received a settlement offer had to pay in order to settle a debt—that is, the settlement amount plus the associated CSA fees. MF 43.

almost two-thirds of Vermont consumers' debts—599 out of 903—were the subject of no settlement offer at all.

While there may be many reasons for these dismal results—including poor performance by CSA, intransigence by creditors, and consumer inability or unwillingness to continue with the CSA program—it was still CSA's legal obligation to have prior reasonable substantiation for its advertising claims, taking into account all of the debts and debtors enrolled. The actual numbers show that even on a *post hac* basis, the Vermont data is completely at odds with what CSA told the public in order to lure consumers to sign up with the company.¹³

National results. The national results data set produced by CSA is insufficient to prove much of anything, for several reasons.

First, that data covers only a brief period of time, encompassing just 12 non-sequential months between August 2006 and October 2007, MF 52, a time period that did not even begin until over two years after the first Vermonters enrolled with CSA. In fact, by August 2006, fully 94 (45.4%) of the total of 207 Vermont customers of CSA had already enrolled with the company, MF 53, so the national data provided by CSA completely misses the time period that is most relevant to almost half of the company's Vermont customers.

¹³ There are two possible explanations for why Defendants might believe they had stronger support for their claims than they did, but both of these involve unfairly inflating consumers' savings, contrary to the FTC principles described in the text. First, CSA calculated savings based on the amount of the debt at the time of *settlement*, rather than at the time of *enrollment*. See *DVA* at 87, MF 49. Even so, CSA itself focused on the amount of the debt at the time of enrollment in its telemarketing script, which stated, "Now, what our company does is called **settlement**. We **dramatically reduce your debt and get you out in 3 years or less!!** Based on \$ _____ (*original amount*) what we'll do is **reduce** your debt down to \$ _____ (*50% of original amount*)." MF 50 (bold and italics in original, underline added for emphasis). Second, Defendant Van Arsdale thought it acceptable to base CSA's claims on only the debts the company *settled*, rather than on all of the debts consumers enrolled. See *DVA* at 200 (CSA's percentage savings claim was based on "just the actual ones [debt settlements] that were accepted"), MF 51.

Second, CSA's claimed national results are completely inconsistent with the FTC principles described above: they include only debts that were settled, not all debts for any period of time; they are based on amounts due at the time of settlement, not at enrollment; and they do not include any of CSA's fees in the calculation of savings.

Third, the only way to evaluate CSA's claimed national results as potential substantiation for its results advertisements is to compare the number of settlements at the advertised level of savings with *all* enrolled debts.¹⁴ However, as noted in the State's Motion of Sanctions Under V.R.C.P. 37(b), filed on November 16, 2011, CSA has never produced that total number of debts—the needed “denominator,” as it were—despite repeated discovery requests and a stipulated Order of the Court that it do so. The fact that CSA has not calculated this “denominator” before is a patently clear indication that it did not have prior, or reasonable, factual substantiation for its claims.

Again, actual results were not consistent with promised results, nor can CSA substantiate its claims with data, this time at the national level.

C. CSA's Results Claims Were Deceptive and Thus Unlawful.

Based on the above data analysis, it is apparent that the three elements of deception under the Consumer Fraud Act, 9 V.S.A. § 2453(a)—misrepresentation, reasonable interpretation and materiality—were present in CSA's advertised results claims.

With respect to the first of those elements, CSA clearly misrepresented the settlement results it obtained for the vast majority of Vermont and national debts. Success rates (as defined by the advertised claims) in the range of 0.7% to 15.4% (the former taking

¹⁴ By way of example, if the national data showed 900 debts successfully settled (*e.g.*, at a 60% savings or more) out of a total of 1,000 debts available to be settled, that would mean that 90% of the debts (900/1,000) were settled consistent with CSA's ads. However, if 900 debts were successfully settled out of a total of 10,000 debts, the

into account fees paid to CSA) mean that CSA negotiated very few Vermont debts at the promised savings. In light of that track record, Vermonters were surely deceived, given that “[i]t is deceptive to make unqualified performance claims that are only true for some consumers, because consumers are likely to interpret such claims to apply to the typical consumer.” *FTC* at 48500 n.575; accord, *FTC v. Five-Star Auto Club, Inc.*, 97 F. Supp. 2d 502, 528-29 (S.D.N.Y. 2000) (it was reasonable for consumers to assume that earnings expressly claimed for multi-level marketing scheme were achieved by typical participant); *National Dynamics Corp. v. FTC*, 492 F.2d 1333, 1335 (2d Cir. 1974), cert. denied, 419 U.S. 993 (1974) (advertising may not make “deceptive use of unusual earnings claims realized only by a few”); *Bailey Employment System, Inc. v. Hahn*, 545 F. Supp. 62, 70 (D. Conn. 1982), aff’d 723 F.2d 895 (2d Cir.1983) (projected earnings claims held deceptive where they did not “bear a reasonable relationship to the average amounts earned in the past by a majority of existing franchisees”); *Porter & Dietsch, Inc. v. FTC*, 605 F.2d 294, 303 (7th Cir. 1979) (deception found where “[t]he typical and ordinary experiences of consumers do not parallel the experiences reported in [advertised] testimonials”). CSA’s advertised results were anything but typical and thus misrepresented the truth of the matter.

As for the second element of deception, in light of the prevailing precedent on the “typicality” that is required of results claims, it was certainly reasonable for consumers to read CSA’s percentage-savings and “debt-free” claims to mean that those were the outcomes they could expect—if not in every case, then for most of them. In this regard, it should be recalled that even if some consumers had a different understanding of the advertising, the

success rate would be only 9% (900/10,000). The difference is crucial: the data could be said to substantiate the advertising only in the first of the two hypotheticals.

claims were still deceptive if they “convey[ed] more than one meaning to reasonable consumers and one of those meanings [was] false.” *Carter v. Gugliuzzi*, 168 Vt. at 56.

Finally, as noted *supra* text 7, the third element—materiality—is satisfied if the representations at issue are express, for those are deemed to be material. Indeed, other than price, what could be more material to consumers, in terms of influencing their decision to enroll with CSA or not, than the savings on their debts that they could expect for their money?

In short, CSA’s website claims were deceptive within the meaning of the Consumer Fraud Act and thus violated the law.

D. CSA’s Advertising Claims Were Unsubstantiated and Thus Unlawful.

As discussed *supra* text 8-9, failure to possess prior reasonable factual substantiation for advertising claims is considered to be an unfair and deceptive trade practice. As the FTC restated in its debt settlement rule commentary, “It is an unfair and deceptive practice to make an express or implied objective claim without a reasonable basis supporting it.” *FTC* at 48500 n. 574.

The FTC has applied this substantiation requirement to debt settlement companies:

When a debt relief service provider represents that it will save consumers a certain amount or reduce the debts by a certain percentage, it also represents, by implication, that this savings claim is supported by competent and reliable, methodologically sound evidence showing that consumers generally who enroll in the program will obtain the advertised results. ... Generally, savings claims should reflect the experiences of the provider’s past customers. ... Similarly, the existence of some satisfied customers does not constitute a reasonable basis.

FTC at 48500 (footnotes omitted).

Given the wide gulf between CSA’s advertised results and its actual outcomes, the question becomes, is it possible that CSA had some other prior, reasonable substantiation to

support its online results claims? As detailed below, the answer from Defendant Van Arsdale's New York deposition testimony is clearly "no," at least as to CSA's initial year of 2004 in Vermont; and for later years, CSA looked to its own national data, which has already been shown to have failed to support those claims.

Consider the question of whether CSA had any reasonable substantiation in the company's early years, starting with the company's founding in 2003. Obviously at that point, CSA had no track record of its own to rely on. Instead, Van Arsdale testified, he looked at what other debt settlement companies were doing. *DVA* at 32-33, MF 54. Asked if he obtained any information from those companies about the percentage savings that consumers were likely to achieve, he stated that the savings "varied from 50, 60, 70, 80, 90." *Id.* at 33. However, when asked whether he had seen "any data or records substantiating these percentages," he replied, "I saw a couple of settlement letters."¹⁵ *Id.* Those letters, he said, were shown to him by an employee of a debt settlement company called Debt XS. *Id.* at 33-34.

Van Arsdale was then asked whether he had any information beyond those specific letters, and he responded, "Online at the time as well, there were other smaller companies that were posting their letters of what they were achieving for their clients." *Id.* at 34. Pressed as to whether he saw "other data besides these letters that would reflect consumer savings," he said, "I don't think so." *Id.* at 35. After describing a "general discussion" he had with someone at Debt XS, Van Arsdale was then asked if he knew about the savings for "the total percentage of consumers" at that company, and he replied, "I didn't inquire about

¹⁵ Later in his deposition, Van Arsdale inexplicably changed "a couple of" letters to "a few hundred." *DVA* at 98, MF 55. Nonetheless, he also clarified that he did not know how many times the savings reflected in those letters were reached, did not ask anyone about that, and did not ask any company how often consumers dropped out of their program, *id.* at 103—although he did put CSA's dropout rate at 60%, *id.* at 104—thus

that.” *Id.* at 36. Finally, Van Arsdale was asked if he had “any other substantiation, independent substantiation for the claims that you advertised on the website back in 2003?” His answer was “No.” *Id.* at 40.

It was not until the year 2005 that CSA “started to get more regular reporting [on settlement results] ... and operations started putting those [data] systems in place.” *Id.* at 81, MF 56. This reporting “may have started in late ’04,” but Van Arsdale became more aware of it late in 2005 through reports he received. *Id.* at 81-82.¹⁶

Defendant Van Arsdale attempts to support his company’s results claims are wholly insufficient. For at least the years 2003-04 and into 2005, the only conceivable support for CSA’s quantitative results claims were some settlement letters from another company. Such anecdotal information cannot establish that advertised savings percentages represented typical or consistent outcomes for CSA’s customers. As for later years, the small percentage of debts for which CSA negotiated savings of 40% or 60% is reflected in its own records, as discussed above..

This lack of substantiation extended to CSA’s “debt free” claims, too. Apart from his general statements, lacking in any detail, that the “debt free in 36 months” claim was chosen based on “industry data” and then on what CSA “saw ... as well,” Van Arsdale admitted that he had no specific figures. *DVA* at 210, MF 57. Asked “What percentage of CSA consumers became debt free in less than 36 months?” he replied, “I do not know that.” *DVA* at 217, MF 58. Asked “Did you have any data to support this claim?” he said, “I knew that clients were settling in three or four months. So I’m assuming there was some data.”

reinforcing the fact that he had nothing but anecdotes on which to base his company’s results claims.

¹⁶ Mr. Van Arsdale was asked if he started getting this “more data” in “late ’05 and in ’06.” He answered, “Correct.” *Id.* at 87.

Id. at 217-18. Nor did he know what percentage of consumers took more than 36 months to settle all of their debts. *Id.* at 218. Again, where the law required there to be prior reasonable substantiation, there was none.

The FTC—and thus Vermont law—patently expect much more in the way of quantitative data to substantiate the kinds of percentage savings claims that CSA used to solicit its customers:

Although providers [*i.e.*, debt settlement companies] may use samples of their historical data to substantiate savings claims, these samples must be representative of the entire relevant population of past customers. Providers using samples must, among other things, employ *appropriate sampling techniques, proper statistical analysis, and safeguards for reducing bias and random error*. Providers may not cherry-pick specific categories of consumers or exclude others in order to inflate the savings.

FTC at 48500 n.577 (emphasis added).

In sum, CSA violated the Consumer Fraud Act by failing to have prior reasonable substantiation of its online results claims.

VII. DEFENDANTS VIOLATED THE CONSUMER FRAUD ACT'S REQUIREMENTS ON THE RIGHT TO CANCEL TELEPHONIC TRANSACTIONS.

A. The Consumer Fraud Act Imposes Specific Requirements with Respect to Consumers' Right to Cancel Telephonic Transactions.

Under the Vermont Consumer Fraud Act, “home solicitation sales” are subject to a three-business-day right to cancel, 9 V.S.A. § 2451a(d). A “home solicitation sale” includes a transaction “solicited or consummated wholly or in part by telephone with a consumer at the residence or place of business or employment of the consumer.” *Id.*

Under 9 V.S.A. § 2454(a)(1), with limited exceptions not pertinent here, “in addition to any right otherwise to revoke an offer, the consumer or any other person obligated for any

part of the purchase price may cancel a home solicitation sale until midnight of the third *business day* after the day on which the consumer has signed an agreement or offer to purchase relating to such sale, or has otherwise agreed to buy consumer goods or services from the seller.” (Emphasis added.) A “business day” is defined as “any calendar day except Saturday, Sunday or any day classified as a holiday under [state law].” 9 V.S.A. § 2451a(e); *accord*, CF 113.01(b). Moreover, “[w]ithin ten [business] days after a home solicitation sale has been cancelled ..., the seller shall tender to the consumer any payments made by the consumer.” 9 V.S.A. § 2454(c)(1). This right to cancel is an extremely important protection for consumers, affording them a “cooling off” period during which they can reconsider their decision to enter into a transaction or contract with a business that they have dealt with only at a distance.

Title 9 V.S.A. § 2454, and, for telephonic sales, the Vermont Attorney General’s Consumer Fraud Rule (CF) 113, available at <http://www.atg.state.vt.us/display.php?smod=131>, describe the kinds of disclosures of this right to cancel that must be made by a seller of goods or services. Under 9 V.S.A. § 2454(b) and CF 113.02, in every telephonic home solicitation sale, the seller must furnish to the consumer, prior to debiting a bank account or otherwise initiating payment, a receipt or contract of sale containing both a short and a multi-paragraph disclosure of the right to cancel, the latter containing the terms of that right. In addition, the seller in a telephonic sale must *orally* inform the consumer of his or her right to cancel the transaction prior to the buyer’s receipt of those written notices. 9 V.S.A. § 2454(b)(2)(D) and CF 113.02(c).

Failure to comply with CF 113 is an unfair and deceptive act and practice in commerce under the Consumer Fraud Act. 9 V.S.A. § 2454(h) and CF 113.05. One remedy

for this failure is described in 9 V.S.A. § 2454(b)(3): “Until the seller has complied with this subsection, the consumer ... may cancel the home solicitation sale by notifying the seller in any manner and by any means of his intention to cancel. The cancellation period of three business days shall begin to run from the time the seller complies with this subsection.” *Accord*, CF 103.02(d) and 103.03. Thus there is no time limit on this important entitlement, affording a strong incentive for businesses to comply strictly with the requirements of the law. Moreover, if a company like CSA has performed any services pursuant to a “home solicitation sale” prior to its cancellation, “the seller shall be entitled to no compensation therefor.” 9 V.S.A. § 2454(d)(7).

Thus, among other things, the Consumer Fraud Act and CF 113 require:

1. Oral as well as written disclosure of the right to cancel.
2. An opportunity to cancel within three business days.
3. An opportunity to cancel by mail.
4. Upon cancellation, payment of a full refund to the consumer.
5. Payment of any required refund within ten business days of cancellation.

It should be stressed that all of these requirements associated with the right to cancel are very specific and not open to variation or revision by any business. Indeed, the Vermont Supreme Court does not approve of attempts to read limitations into the Consumer Fraud Act that do not expressly appear on the face of the statute. *See State v. Internat’l Collection Service, Inc.*, 156 Vt. 540 (1991) (rejecting argument that Consumer Fraud Act did not authorize Attorney General to sue business for engaging in unfair or deceptive acts or practices against other businesses, rather than against individual consumers).

B. CSA’s Cancellation Notice Did Not Meet the Statutory Requirements.

As a threshold matter, all of Defendants’ transactions with Vermont consumers involved a telephone conversation between the consumer and a CSA representative to solicit

the consumer's interest in entering into a service contract with the company and to firm up the details of that agreement. MF 59. As such, they were "home solicitation sales" within the meaning of the Consumer Fraud Act and thus required a three-business-day right to cancel as prescribed by the Act and CF 113.

However, in no fewer than five respects CSA failed to comply strictly with its obligations relating to the right to cancel and thus violated the Consumer Fraud Act, 9 V.S.A. §§ 2453(a) and 2454, and CF 113.

First, CSA's telephonic marketing script contained no oral disclosure of any right to cancel. MF 60.

Second, CSA's written notice of the right to cancel, which appeared in its standard Agreement, set out a right to cancel that lasted only until "midnight of the third day after the date of the transaction," MF 61—in other words, three calendar days, not the statutory three *business* days, after that date. The difference had real importance: over a weekend, it meant that a right to cancel that should have lasted for five calendar days (three business days and two weekend days) was two days shorter than it should have been, and over a holiday weekend it was shorter by three days.

Third, CSA compelled consumers both to mail *and* to fax their cancellation request, rather than simply to mail, deliver, *or* telegraph the request. MF 62. That imposed a significant burden on their customers, particularly in rural Vermont, to access a fax machine if they wanted to cancel.

Fourth, CSA's contract with consumers stated that consumers were "**OBLIGATED TO PAY CREDIT SOLUTIONS THAT PORTION OF THE *TOTAL FEES ALREADY EARNED* BY COMPANY IN ACCORDANCE WITH PARAGRAPH 13 OF THIS**

AGREEMENT.” MF 63 (capitals and bold in original, italics added). Paragraph 13 of the contract between consumers and CSA in turn described the installment payments to be made by the consumer to Credit Solutions of America, including the service fees due the company. MF 64. The first of these installments was often due as early as the date the consumer signed the Agreement, or, in the absence of a signature, the date of the Agreement itself.¹⁷ MF 65.

That first month’s payment could be substantial. For example, Vermont consumer B.M.’s first monthly payment of \$538.13 in fees was due, under Paragraph 13 of his contract with CSA, on the same day as the date on the contract and thus was “already earned by the company” and not refundable. MF 67. As a result, the consumer’s entitlement to a full refund was substantially compromised.

Fifth, CSA’s written right-to-cancel notice provided that the company had 30 days to pay a refund in the event of a cancellation, MF 68, thus substantially lengthening the repayment interval from the statutory 10 business days, to the consumer’s detriment.

In short, CSA systemically violated its right-to-cancel-related obligations under Vermont law and is now required to provide a full refund to any consumer who manifests an intention to cancel.

VIII. DEFENDANTS VIOLATED THE CONSUMER FRAUD ACT BY FAILING TO COMPLY WITH THE VERMONT DEBT ADJUSTERS ACT.

As noted above, one of the alternative tests for determining whether a trade practice is unfair under the Consumer Fraud Act is “whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by

¹⁷ Of the 207 Vermont consumer files analyzed for this Motion, fully 145 had a first payment due on the same date as the contract was signed (or on the printed contract date, if there was no signature date). MF 66.

statutes, the common law, or otherwise—whether, in other words, it is within at least the penumbra of some common-law, statutory, or other established concept of unfairness.” *Christie v. Dalmig*, 136 Vt. at 601 (quoting *FTC v. Sperry & Hutchinson Co.*, 405 U.S. at 244 n.5). Here, the State alleges that Defendants failed to comply with the Vermont Debt Adjusters Act, 8 V.S.A. chapter 83, 8 V.S.A. ch. 133,¹⁸ a statute designed in large part to protect consumers, and that Defendants’ non-compliance in turn amounted to an unfair trade practice.

A. CSA Was a “Debt Adjuster” Subject to the Debt Adjusters Act.

At all times relevant to this lawsuit, CSA’s business fell within the following definition of “debt adjustment” in 8 V.S.A. § 4861(2) as that definition existed during the time period relevant to this case¹⁹ and was thus subject to the provisions of the Debt Adjusters Act:

“Debt adjustment” means making a contract with a debtor whereby the debtor agrees to pay a sum or sums of money periodically and the other party to the contract distributes, supervises, coordinates, *negotiates*, or controls the distribution of such money or evidences thereof among one or more of the debtor’s creditors in full or partial payment of obligations of the debtor. For purposes of this chapter, engaging in debt adjustment in this state shall include: (A) soliciting debt adjustment business from within this state, whether by mail, by telephone, by electronic means, or by other means regardless of whether the debtor resides within this state or outside this state; (B) soliciting debt adjustment business with an individual residing in this state, whether by mail, by telephone, by electronic means, or by other means; or (C) entering into, or succeeding to, a debt adjustment contract with an individual residing in this state. [Emphasis added.]

Under CSA’s business model, echoing the language of the statute, (1) “the debtor agrees to pay a sum or sums of money periodically,” and (2) CSA (“the other party to the

¹⁸ Former chapter 133 of title 8 V.S.A., consisting of sections 4861-4876, was recodified in 2010 as chapter 83 of the same title, comprising sections 2751-2766. Act 137 (2009 Adj. Sess.), § 3.

¹⁹ The quoted definition was amended in 2010 simply “to clarify existing law,” *see* S. 278 as passed by the House and Senate, § 29(c), <http://www.leg.state.vt.us/docs/2010/bills/Passed/S-278.pdf>; but in any event, the current definition continues to encompass CSA’s core activity, which is to “negotiate ... the distribution of money or evidences thereof among one or more of the debtor’s creditors in full or partial payment of obligations of the debtor.”

contract”) “negotiates ... the distribution of such money ... among one or more of the debtor’s creditors in full or partial payment of obligations of the debtor.”

The first of these elements—the debtor’s agreement to make periodic payments—is reflected in the Estimated Personal Savings Plan for Payments to Creditors (“the Plan”) set out in the CSA Customer Enrollment Package sent to all customers of the company. MF 69. As noted in the example reprinted *supra* text 29, the Plan includes a chart that contains information on the total dollar amount of the consumer’s enrolled debts, the fees due CSA, and total savings. Pertinent to the statutory issue at hand, it also states the amount of “Minimum Personal Saving Payments After Credit Solutions Fee is Paid,” to be deposited by the consumer into his or her bank account. These payments, as noted at the bottom of the sheet, are “the minimum²⁰ suggested for payoff of your enrolled account ... Credit Solutions highly recommends that any additional funds which may become available be allocated towards your personal savings account.” MF 70 (emphasis in original). These consumer payments are an essential element of the CSA program, as described by the company: “When the client has the available funds to settle an account, [CSA] contacts the creditor and asks that a settlement be negotiated in the amount that the customer has saved.” MF 71; *see also* Client Service Agreement ¶ 12 (consumer agrees to budget a set amount per month for ultimate distribution to creditors). MF 72.

The second element—negotiation of the distribution of such money among one or more of the debtor’s creditors in full or partial payment of the debtor’s obligations—exactly describes CSA’s core service. CSA offers to negotiate with a consumer’s creditors to reduce the principal amount of the consumer’s debts, thus purportedly achieving the

²⁰ A later version of the Estimated Personal Savings Plan dropped that title and highlighted the word “minimum” by italicizing and bolding it (“*minimum*”).

percentage savings described earlier in this Memorandum. As the company has acknowledged, CSA “provides consumer debt *negotiation* and settlement services. [CSA] customers enroll certain unsecured accounts with [CSA] and [CSA] *negotiates* for settlement offers on those accounts.” MF 73 (emphasis added). Once one or more debt settlements have been negotiated by CSA and accepted by the consumer, the agreed-upon funds are thus distributed by the consumer to or among the creditors according to the settlement terms.²¹ MF 74.

When interpreting a statute, the courts “first rely upon the plain language of the law as a means of determining legislative intent.” *Nichols v. Hofmann*, 2010 Vt. 36, ¶ 7, 188 Vt. 1 (citing *Delta Psi Fraternity v. City of Burlington*, 2008 VT 129, ¶ 7, 185 Vt. 129). “If that plain language resolves the conflict without doing violence to the legislative scheme, there is no need to go further” *Id.* (quoting *Lubinsky v. Fair Haven Zoning Bd.*, 148 Vt. 47, 49 (1986)). Moreover, in this case, the licensing agency for debt adjusters, the Vermont Department of Banking, Insurance, Securities and Health Care Administration (BISHCA), has opined that CSA meets the definition of debt adjuster under the law, MF 75, which is significant because “[t]he interpretation of an agency charged with the administration of a statute is entitled to substantial deference, if it is a sensible reading of the statutory language, ... and if it is not inconsistent with the legislative history.” *Internat’l Collection Service*, 156 Vt. at 545-46 (quoting *Lawrence County v. Lead-Deadwood School Dist. I*, 469 U.S. 256, 262 (1985)).

²¹ Because CSA has expressly acknowledged that it negotiates with consumers’ creditors for the payment of a reduced debt amount, there is no need to resort to rules of construction to try to discern what the term “negotiates” means in the Debt Adjusters Act.

Here, nothing in the Debt Adjusters Act requires CSA itself to handle the consumer's settlement funds. The "distribution" of such funds need not be effected directly by CSA in order for the company to be considered a debt adjuster. It is simply the consumer's agreement to make periodic payments and CSA's negotiation of a reduced principal amount due on the consumer's debt that characterizes a debt adjuster under a plain-language reading of Vermont law; and CSA meets that definition.

B. CSA Violated At Least Seven Requirements of the Debt Adjusters Act.

The Debt Adjusters Act goes on to impose a series of pro-consumer obligations on companies subject to the law. These obligations first include having to obtain a license from BISHCA, 8 V.S.A. § 2752, to ensure, among other things, that the company and those who control it have "the financial responsibility, experience, character, and general fitness ... [to] command the confidence of the community and warrant belief that the business will be operated honestly, fairly, and efficiently within the purposes of [the law]." 8 V.S.A. § 2756. However, CSA never obtained a license. MF 76.

Other obligations under the Act designed to protect Vermont consumers include licensees' having to (1) post a bond to secure the company's performance of its obligations as a licensee, 8 V.S.A. § 2755; (2) submit an annual report containing, among other things, the number of new consumer contracts entered into with Vermont consumers, contracts completed, contracts cancelled, and total contracts in force, 8 V.S.A. § 2757a(a)(2)—all factors relevant to the success of the licensee's program; (3) provide consumers with written contracts in a form approved by BISHCA and containing specified disclosures, including the fact that debt adjustment plans are not suitable for all debtors, 8 V.S.A. § 2759(a)-(b); (4) afford a three-business-day right to cancel the contract and provide disclosures of that right,

8 V.S.A. § 2759, identical to those required by the Consumer Fraud Act; and (5) limit their fee for services to a \$50.00 initial setup fee plus ten percent of any payment received by the company for distribution to creditors, 8 V.S.A. § 2762. Finally, no one other than a licensee may use the term “debt reduction” in any public advertisement. 8 V.S.A. § 2760b(c).

In fact, CSA failed to comply with any of these requirements. CSA did not post the requisite bond. MF 77. The company did not submit an annual report. MF 78. It did not disclose in its contract that debt adjustment plans are not suitable for all debtors. MF 79. It did not comply strictly with the right-to-cancel requirement for the same five reasons as it failed to comply with the right-to-cancel disclosure requirements of the Consumer Fraud Act, *see supra* text 26-28. MF 80. And it clearly did not limit its fee for services to a \$50.00 initial setup fee plus ten percent of any payment received by the company for distribution to creditors. MF 81. Moreover, CSA did use the prohibited term “debt reduction” in many of its public advertisements. MF 82.

It should be noted, finally, that most of the provisions of the Debt Adjusters Act relevant to this case share with the Consumer Fraud Act the objective of protecting Vermonters from financial harm, in this case at the hands of a regulated industry. The limit on fees to be charged is clearly one such provision, as is the requirement of a contractual disclosure that debt adjustment plans are not suitable for all debtors, the requirement of a three-day right to cancel properly disclosed, and, to a lesser but still extant degree, the bonding and annual report provisions and the restriction on the use of the term “debt reduction” in any public advertisement. As such, the statute’s goals are remedial, warranting a liberal construction in the application of the law to CSA. *See Carter v. Fred’s*

Plumbing & Heating, Inc., 174 Vt. 572, 574 (mem. 2002) (“Remedial statutes are entitled to liberal construction.”); *see also* cases cited *supra* text 6.

IX. DEFENDANT VAN ARSDALE IS PERSONALLY LIABLE FOR CSA’S VIOLATIONS OF LAW.

A. Vermont Law Supports Personal Liability for Consumer Fraud Violations.

Under Vermont law, a corporate officer may be held derivatively liable for consumer fraud where he or she has directly participated in the unfair or deceptive acts, directly aided the actor, or has a principal/agent relationship with the actor. *See State v. Stedman*, 149 Vt. 594, 598 (Vt. 1988). In *Stedman*, the Supreme Court acknowledged that such derivative liability can also extend to a principal who “has engaged in, is aware of, or has condoned deceptive acts of his agents.” *Id.* (citing *Jackson v. Harkey*, 704 P.2d 687, 692 (Wash. App. 1985)).

Federal courts have taken a similar approach to derivative liability. For example, in *FTC v. Amy Travel Service, Inc.*, 875 F.2d 564, 573-74 (7th Cir. 1989), the FTC sued three telemarketing companies and two of their owner-officers for deceptively marketing and selling “vacation certificates.” The individual defendants had developed the basic script used by the companies’ telemarketers, which the trial court found to be deceptive. As is alleged here, the individual defendants “were certainly aware of the misrepresentations contained in them.” 875 F.2d at 574. The court held that since the officers had both the authority to control their companies and some knowledge of the challenged practices, they were personally liable. *See* 875 F.2d at 573. *Accord*, *Consumer Protection Division v. Morgan*, 874 A.2d 919, 949 (Md. App. 2005) (“We hold that the Consumer Protection Division may hold individuals jointly and severally liable for restitution for the Consumer

Protection Act violations of corporations, when the Division proves that (1) the individual participated directly in or had authority to control the deceptions or misrepresentations, and (2) the individual had knowledge of the practices.”)

Authority to control a company, in turn, “can be evidenced by active involvement in business affairs and the making of corporate policy, including assuming the duties of a corporate officer.” *Amy Travel*, 875 F.2d at 573. As for the knowledge requirement, that may be satisfied by demonstrating that the individual had “actual knowledge of material misrepresentations, reckless indifference to the truth or falsity of such misrepresentations, or an awareness of a high probability of fraud along with an intentional avoidance of the truth.” *Id.* at 574 (citation omitted). However, it need not be shown that the person intended to defraud consumers. *Id.*

This view of officer liability is consistent with decisions in other states holding that officers who have not themselves made deceptive representations may be held liable for unfair or deceptive acts and practices by their corporations where they have either knowingly entered into the deceptive scheme, see *Schmidt Enterprises, Inc. v. State*, 354 N.E.2d 247, 253 (Ind. App. 1976); established the company policy, see *Moy v. Schreiber Deed Security Co.*, 535 A.2d 1168, 1171 (Pa. Super. Ct. 1988), and *State ex rel. Medlock v. Nest Egg Society Today, Inc.*, 348 S.E.2d 381, 385-86 (S.C. App. 1986); or approved of promotional materials that were deceptive, see *Grayson v. Nordic Construction Co., Inc.*, 599 P.2d 1271, 1274 (Wash. 1979).

Finally, in an action alleging involvement in unfair or deceptive practices by corporate owner-officers, the Chittenden Superior Court denied a motion to dismiss filed by the individual defendants based on allegations that they had knowledge or control of the

wrongful conduct at issue. *See State v. Vacation Break U.S.A., Inc., et al.*, No. S353-97 CnC (Chittenden Super. Ct., Mar. 11, 1998) (Opinion and Order at 3) (“corporate officers and directors are liable for tortious acts the corporation commits under their direction or with their participation.”). Noting that according to the complaint, the corporate officers “ha[d] known of or controlled” the company’s allegedly unfair and deceptive acts, the Court in that case denied the individual defendants’ motion to dismiss. *Id.* at 3-4.

B. Defendant Van Arsdale Is Personally Liable for CSA’s Violations of Law.

Here, as noted *supra* text 4, Defendant Van Arsdale founded CSA and served as its CEO, Director and Registered Agent until November 2006, as well as resuming his positions as CEO and Registered Agent of CSA in December 2007 and founding CSA’s successor limited liability corporation. However, his role at CSA went well beyond those titles.

First, Defendant Van Arsdale has acknowledged that he had authority over CSA’s website content and was aware of the company’s results claims at or shortly after they appeared on the website, MF 83. Indeed, his “research” into the debt settlement industry—such as it was—led to the inclusion of percentage savings claims on the company’s website, *DVA* at 32-40, a website that Mr. Van Arsdale himself helped put together, *DVA* at 37, 39. MF 84.

Second, Defendant Van Arsdale was aware of CSA’s right to cancel and related notifications from their inception. MF 85. Not only that, but he helped create, approved, and had the authority to change any part of, CSA’s enrollment package, *DVA* at 42-43, which package contained the right-to-cancel rules and procedures challenged in this lawsuit. MF 86. Similarly, Mr. Van Arsdale reviewed, approved, and retained the authority to change the telephone scripts used by CSA, *DVA* at 41-42, MF 87, which scripts omitted the oral notice of the right to cancel mandated by Vermont statute.

Third, Defendant Van Arsdale was aware of Vermont's debt adjuster licensing law on or about the time it became effective. MF 88.

Based on the above, Defendant Van Arsdale is personally liable for CSA's conduct with respect to the company's online results claims, its consumer right-to-cancel policies, and its failure to comply with Vermont's debt adjusters statute, because he had the requisite authority and knowledge of that conduct, as well as direct involvement in it (although such involvement is not strictly needed to establish liability).

X. APPROPRIATE RELIEF

Once the liability of Defendants is established, the issue of appropriate relief must be addressed. The Consumer Fraud Act authorizes the Court to render "any" temporary or permanent relief as may be in the public interest, including consumer restitution, civil penalties of up to \$10,000 per violation, injunctive relief and attorney's fees and costs. 9 V.S.A. § 2458(b).

A. Injunctive Relief

The State has represented that CSA is no longer doing business in Vermont or with Vermont consumers. However, "[i]t is settled that an action for an injunction does not become moot merely because the conduct complained of has terminated, if there is a possibility of recurrence[.]'" *Id.* (quoting *Allee v. Medrano*, 416 U.S. 802, 810 (1974)). Otherwise "the defendant is free to return to his old ways.'" *Id.* (quoting *U.S. v. W.T. Grant*, 345 U.S. 629, 632 (1953), and citing *Beneficial Corp. v. FTC*, 542 F.2d 611, 617 (3d Cir. 1976) (court may bar prior deceptive practice if practice could be resumed), and *Fedders Corp. v. FTC*, 529 F.2d 1398, 1403 (2d Cir.1976) (injunctive relief may extend to discontinued deceptive practice where public interest requires)).

As a result, it is appropriate for the Court to order either that Defendants not conduct any future debt settlement or similar business in Vermont, or, in the alternative, that they (1) not advertise the savings or other results it can achieve unless they first possess reasonable and specific factual substantiation that those results represent the typical outcome for their customers, using a calculation based on all debts enrolled, the amounts due at the time of enrollment, and the inclusion of service fees; (2) strictly comply with Vermont's right-to-cancel requirements as set out in 9 V.S.A. § 2454 and CF 113; and (3) first obtain a state debt adjuster's license and comply with all requirements of the Vermont Debt Adjusters Act. The Court will enjoin Defendants from conducting any debt settlement or similar business in Vermont unless and until they obtain leave of the Court.

B. Consumer Refunds and Other Monetary Relief

Vermont consumers who enrolled with CSA were both deceived by the company as to the debt-reduction results they could expect to achieve, and denied their statutory right to cancel. Accordingly, Defendants will be required, jointly and severally, to provide prompt and full refunds of all as-yet-unrefunded amounts received from Vermont consumers.

C. Civil Penalties

The Consumer Fraud Act, 9 V.S.A. § 2458(b), authorizes the imposition of civil penalties in an amount not to exceed \$10,000 per violation. Each online results claim—of which there were at least 347, measured by just website revisions, MF 31—and each one of CSA's 207 Vermont customers represents a separate violation. *See, e.g., People v. Bestline Products, Inc.*, 132 Cal. Rptr. 767, 795 (1976) (one violation per solicitee); *State ex rel. Corbin v. United Energy Corp. of America*, 725 P.2d 752 (Ariz. Ct. App. 1986) (permitting maximum penalty per victim per violation); *see also State v. Menard, Inc.*, 358 N.W.2d 813, 815 (Wis.

Ct. App. 1984), and *May Dept. Stores Co. v. State ex rel. Woodard*, 863 P.2d 967, 975 (Colo. 1993) (“transaction” under consumer fraud statute means one advertisement in one media outlet per day).

Defendants’ unfair and deceptive practices were substantial and widespread enough to warrant the imposition of significant civil penalties, both as a sanction for Defendant’s conduct and as a deterrent to similar conduct by them and others in the future. The State proposes a civil penalty of \$1,000 for each per-consumer violation, for a total of \$207,000, to be imposed, jointly and severally, on CSA and Defendant Van Arsdale. However, because of the extent and breadth of Defendants’ fraudulent conduct, the Court believes that the maximum penalty of \$2.07 million (\$10,000 times 207 consumers) is appropriate,

D. Fees and Costs

The Consumer Fraud Act, 9 V.S.A. § 2458(b), also provides for “an order requiring reimbursement to the State of Vermont for the reasonable value of its services and its expenses in investigating and prosecuting [this] action.” The Court will order CSA and Defendant Arsdale, jointly and severally, to pay the State’s reasonable fees and costs in this matter. The State will submit an affidavit to the Court setting out the hours logged by its legal staff and recommended reimbursement rates within 30 days of this Order.

ORDER

The State’s Motion for Summary Judgment on Counts 1, 2 and 4 is *granted*. The State will file a proposed order, consistent with this decision within ten days.

Dated at Montpelier, Vt., March 5, 2012,


Michael S. Kupersmith
Superior Judge