

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO**

FEDERAL TRADE COMMISSION,

Plaintiff,

v.

DIGITAL FORENSICS CORPORATION, LLC, a
limited liability company;

1ST ALL DATA RECOVERY LLC, a limited
liability company, also dba DIGITAL FORENSICS
CORP;

1ST ALL FILE RECOVERY USA, INC., a
corporation, also dba DIGITAL INVESTIGATION,
FILE RECOUP; CYBER BLACKMAIL 911; and
DIGITAL FORENSICS;

I & D BELKIN LLC, a limited liability company,
also dba DATA RECOVERY SERVICES and
DIGITAL FORENSICS CORP;

REMOTE BACKUP CORP, LLC, a limited liability
company, also dba DIGITAL CYBER FORENSICS
INVESTIGATION;

DIGITAL CYBER FORENSICS
INVESTIGATIONS LLC, a limited liability
company, also dba CYBER INVESTIGATION;

CYBER DIGITAL FORENSICS RESPONSE LLC,
a limited liability company;

1ST ALL INVESTMENTS, LLC, a limited liability
company;

SALON PLACE LLC, a limited liability company;

VPR ACADEMY LLC, a limited liability company;

FILED UNDER SEAL

Case No. _____

**MEMORANDUM IN SUPPORT OF
PLAINTIFF'S MOTION FOR *EX*
PARTE TEMPORARY
RESTRAINING ORDER WITH
ASSET FREEZE AND ORDER TO
SHOW CAUSE WHY
PRELIMINARY INJUNCTION
SHOULD NOT ISSUE**

21111 CHAGRIN INVESTMENTS LLC, a limited liability company;

4350 RENAISSANCE LLC, a limited liability company; and

DMITRY BELKIN, individually and as an officer and/or owner of DIGITAL FORENSICS CORPORATION, LLC; 1ST ALL DATA RECOVERY LLC; 1ST ALL FILE RECOVERY USA, INC.; I & D BELKIN LLC; REMOTE BACKUP CORP, LLC; DIGITAL CYBER FORENSICS INVESTIGATIONS LLC; CYBER DIGITAL FORENSICS RESPONSE LLC; 1ST ALL INVESTMENTS, LLC; SALON PLACE LLC; VPR ACADEMY LLC; 21111 CHAGRIN INVESTMENTS LLC; and 4350 RENAISSANCE LLC,

Defendants.

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	STATEMENT OF FACTS	2
	A. Defendants	2
	B. Sextortion Background	6
	C. Defendants' Deceptive Marketing of Unnecessary Sextortion Services	8
	D. Defendants Fail to Perform Promised Phase 1 Services.....	11
	E. Defendants Upsell Phase 2 Services and Fail to Deliver Them.....	13
	F. Defendants Do Not Honor Their Refund Policy.....	15
	G. Defendants Ignore and Suppress Complaints	15
	H. Defendants Disseminate Fake Positive Reviews	18
	I. Defendants Abuse and Manipulate the Judicial Process.....	19
III.	ARGUMENT	20
	A. The Court Has the Authority to Grant the Requested Relief	20
	B. The FTC Meets the Standard for Preliminary Injunctive Relief.....	21
	1. The FTC Is Likely to Succeed on the Merits.....	22
	2. Corporate Defendants Act as a Common Enterprise and Are Jointly and Severally Liable for Each Other's Violations.....	27
	3. Belkin Is Individually Liable for Injunctive and Monetary Relief.....	29
	4. Irreparable Harm Exists	30
	5. The Balance of Equities Mandates Preliminary Injunctive Relief.....	31
	6. Injunctive Relief Will Serve the Public Interest.....	31
	C. An <i>Ex Parte</i> TRO with Additional Equitable Relief Is Necessary to Provide Final Effective Relief	32
	1. Conduct Relief Is Necessary to Stop Ongoing Consumer Harm.....	32
	2. An Asset Freeze Is Critical to Preserve the Possibility of Final Relief	33
	3. Appointment of a Temporary Receiver Is Appropriate.....	34
	4. It Is Necessary to Authorize Immediate Access to Defendants' Business Premises and Order Preservation and Production of Records	35
	5. <i>Ex Parte</i> Issuance Is Warranted	35
IV.	CONCLUSION	36

TABLE OF AUTHORITIES

Cases

<i>Chefs' Warehouse Midwest, LLC v. CSX Transp., Inc.</i> , No. 1:17-CV-555, 2017 WL 3872484 (S.D. Ohio Sept. 5, 2017).....	6
<i>City of New York v. Golden Feather Smoke Shop, Inc.</i> , 597 F.3d 115 (2d Cir. 2010).....	30
<i>E.V. v. Raycraft</i> , No. 4:25-CV-2069, 2025 WL 2938594 (N.D. Ohio Oct. 16, 2025).....	21
<i>EOG Res., Inc. v. Lucky Land Mgmt., LLC</i> , 134 F.4th 868 (6th Cir. 2025).....	21
<i>First Tech. Safety Sys., Inc. v. Depinet</i> , 11 F.3d 641 (6th Cir. 1993).....	35
<i>FTC v. 1st Beneficial Credit Servs., LLC</i> , No. 1:02 CV 1591 (N.D. Ohio Aug. 14, 2002)	34
<i>FTC v. 90I07-4021 Quebec, Inc.</i> , No. 1:08 CV 1051 (N.D. Ohio Apr. 25, 2008).....	34
<i>FTC v. Affordable Media</i> , 179 F.3d 1228 (9th Cir. 1999).....	31
<i>FTC v. Amy Travel Service, Inc.</i> , 875 F.2d 564 (7th Cir. 1989).....	21, 23, 29
<i>FTC v. BlackRock Services, Inc.</i> , 8:25-cv-00363, Dkt. 2-1 (C.D. Cal. Feb. 27, 2025).....	35
<i>FTC v. Butterworth Health Corp.</i> , 121 F.3d 708 (Table), 1997 WL 420543 (6th Cir. July 8, 1997) (per curiam).....	21
<i>FTC v. Campbell Cap. LLC</i> , 2018 U.S. Dist. LEXIS 186728 (W.D.N.Y. Oct. 24, 2018)	31
<i>FTC v. Credit Bureau Ctr., LLC</i> , 937 F.3d 764 (7th Cir. 2019)	29
<i>FTC v. Credit Glory LLC</i> , CV-26-05387-PHX-SPL, Dkt. 18 (D. Ariz. Aug. 4, 2026).....	35
<i>FTC v. E.M.A. Nationwide, Inc.</i> , 767 F.3d 611 (6th Cir. 2014).....	22, 23, 27, 29, 36
<i>FTC v. Elegant Sols., Inc.</i> , No. 20-55766, 2022 WL 2072735 (9th Cir. June 9, 2022)	33
<i>FTC v. Foreclosure Sols., LLC</i> , No. 1:08 CV 1075, 2008 WL 11380125 (N.D. Ohio Nov. 21, 2008)	21, 22, 25, 33
<i>FTC v. Freecom Commc'ns, Inc.</i> , 401 F.3d 1192 (10th Cir. 2005).....	29
<i>FTC v. Hanson Pubs., Inc.</i> , No. 1:02 CV 2205 (N.D. Ohio Nov. 12, 2002).....	34
<i>FTC v. Int'l Computer Concepts, Inc.</i> , 1994 WL 730144 (N.D. Ohio Oct. 24, 1994)	22, 25, 31, 34
<i>FTC v. Int'l Computer Concepts, Inc.</i> , No. 5:94-CV-1678 (N.D. Ohio Aug. 17, 1994)	34, 36
<i>FTC v. Mallett</i> , 818 F. Supp. 2d 142 (D.D.C. 2011)	31
<i>FTC v. Mazzoni & Son, Inc., d/b/a EDI Healthclaims Network, et al.</i> , No. 1:06 CV 2385 (N.D. Ohio Oct. 3, 2006)	34
<i>FTC v. NHS Sys., Inc.</i> , 936 F. Supp. 2d 520 (E.D. Pa. 2013).....	29
<i>FTC v. One or More Unknown Parties Deceiving Consumers</i> , No. 5:20-cv-2494 (N.D. Ohio Nov. 5, 2020)	34
<i>FTC v. Repair All PC, LLC, et al.</i> , No. 1:17-cv-00869-DAP (N.D. Ohio Apr. 24, 2017)	34
<i>FTC v. Solar Michigan, Inc.</i> , 1988-2 Trade Case. (CCH) P68,339 (E.D. Mich. 1988).....	33
<i>FTC v. Wash. Data Res.</i> , 856 F.Supp.2d 1247 (M.D. Fla. 2012)	27, 29
<i>FTC v. World Wide Factors Ltd.</i> , 882 F.2d 344 (9th Cir. 1987).....	30, 31
<i>In re Southwest Sunites, Inc.</i> , 105 F.T.C. 7, 149 (1985), <i>aff'd</i> 785 F.2d 1431 (9th Cir. 1986).....	25
<i>McGirr v. Rehme</i> , 891 F.3d 603 (6th Cir. 2018).	31
<i>Mullins v. City of New York</i> , 626 F.3d 47 (2d Cir. 2010)	6
<i>Six Clinics Holding Corp., II v. Cafcomp Systems, Inc.</i> , 119 F.3d 393 (6th Cir. 1997)	22
<i>Thompson Medical Co.</i> , 104 F.T.C. 648 (1984), <i>aff'd on other grounds</i> [1986–1 Trade Cases ¶ 67,103], 791 F.2d 189 (D.C. Cir. 1986), <i>cert. denied</i> , 479 U.S. 1086 (1986))	22

<i>United States v. Diapulse Corp of Am.</i> , 457 F.2d 25 (2d Cir. 1972).....	30
--	----

Statutes

15 U.S.C. § 45(a)	22
15 U.S.C. § 53(b)	20
15 U.S.C. § 57b	33
15 U.S.C. § 57b(b)	21
15 U.S.C. § 6821(a)(2).....	23
15 U.S.C. § 6827(2)	24
Pub. L. No. 119-12, § 146, 139 Stat. 55 (2025).....	7

Rules

16 C.F.R. § 310.3(a)(2)(iii)	23
16 C.F.R. § 310.3(a)(4)	23
16 C.F.R. § 465.2(a)(1)	26
16 C.F.R. § 465.2(b)(2)	27

NOTES ON CITATIONS¹

1. References to “Agarwal Decl.” refer to the Declaration of FTC Forensic Accountant Roshni C. Agarwal.
2. References to “Smedley Decl.” refer to the Declaration of FTC Investigator Tiffany Smedley.
3. References to “Dilworth Decl.” refer to the Declaration of Ericka Dilworth, the Vice President of Operations for the Better Business Bureau Serving Greater Cleveland.
4. References to “Coffren Decl.” refer to the Declaration of Lauren Coffren, the Executive Director of the Exploited Children Division at The National Center for Missing and Exploited Children.
5. References to “Raffile Decl.” refer to the Declaration of Paul Raffile.
6. References to “Tolok Decl.” refer to the Declaration of Mark Tolok.
7. References to “Lydick Decl.” refer to the Declaration of Roberta Lydick.
8. References to “Boyer Decl.” refer to the Declaration of Trevor Boyer.
9. References to “Lopaz Decl.” refer to the Declaration of Trevor Lopaz.
10. References to “Snell Rule 65(b)(1) Decl.” refer to the Rule 65(b)(1) Certification and Declaration of Maris K.V. Snell in support of Plaintiff’s Motion for *Ex Parte* Temporary Restraining Order with Asset Freeze and Order to Show Cause Why Preliminary Injunction Should Not Issue, filed concurrently herewith.

¹ Citations to exhibit page numbers, herein, refer to the pagination stamped in the lower righthand corner of all exhibits.

I. INTRODUCTION

A sextortion victim, panicked, searches online for help. One of the first results on the search engine promises expert investigators who will take over communications with the attacker, trace the sextortionist's identity and location, and make the threat stop — for thousands of dollars. The victim pays for these “sextortion assistance services.” Nothing happens.

That is Defendants' scheme. Operating through a web of interrelated corporate entities under the control of Defendant Dmitry Belkin, Defendants have preyed on thousands of sextortion victims since at least 2020. Defendants falsely promise consumers a multi-step investigative process to stop sextortion attacks. In reality, they perform little or none of the promised services—blocking sextortionists without communicating, fabricating investigative reports with fake chat logs and invented GPS coordinates, and pressuring victims to pay thousands more for a second phase they also fail to deliver. When victims complain, Defendants delay refunds until contractual deadlines expire and condition any refund on confidentiality agreements requiring removal of negative reviews. To maintain the appearance of legitimacy, Defendants flood review platforms with fake five-star ratings generated through paid strangers and overseas employees.

Since 2023, Defendants have taken in at least \$60 million from thousands of consumers. Defendants have dissipated millions through international wire transfers, luxury purchases, and over \$38 million in personal credit card charges. Defendants have also falsified records submitted in response to a law enforcement subpoena and systematically intimidated former employees and consumers into silence.

Defendants' conduct violates Section 5(a) of the FTC Act, 15 U.S.C. § 45(a); the Telemarketing Sales Rule (“TSR”), 16 C.F.R. Part 310; the Gramm-Leach-Bliley Act (“GLB

Act”), 15 U.S.C. §§ 6801-6809, 6821-6827; and the FTC’s Trade Regulation Rule on the Use of Consumer Reviews and Testimonials (“Reviews and Testimonials Rule”), 16 C.F.R. Part 465. For these violations, Plaintiff Federal Trade Commission (“FTC” or “Commission”) respectfully requests *ex parte* temporary restraining order (“TRO”) that: (1) enjoins Defendants’ unlawful practices; (2) freezes Defendants’ assets; (3) appoints a temporary receiver; (4) grants immediate access to Defendants’ business premises and records; and (5) orders Defendants to show cause why a preliminary injunction should not issue. Defendants have repeatedly taken action to destroy and conceal evidence of their unlawful scheme, provide falsified evidence to law enforcement and thousands of customers, and quickly dissipate corporate assets, including through international transfers. Given Defendants’ history there is good reason to believe Defendants would disregard the requirements of a court order, therefore the FTC seeks this preliminary relief *ex parte*. These measures are necessary to prevent continued consumer harm and Defendants’ destruction of evidence, and to preserve the Court’s ability to return money to consumers.

II. STATEMENT OF FACTS

A. Defendants

Individual Defendant Dmitry Belkin (“Belkin”) owns and controls the Corporate Defendants.² Belkin is the “mastermind” behind Defendants’ scheme, according to Defendants’

² “Corporate Defendants” collectively refers to Defendants Digital Forensics Corporation, LLC (“DFC”); 1st All Data Recovery LLC (“1st All Data Recovery”); 1st All File Recovery USA, Inc. (“1st All File Recovery”); I & D Belkin LLC (“I & D Belkin”); Remote Backup Corp, LLC (“Remote Backup Corp”); Digital Cyber Forensics Investigations LLC (“Cyber Investigation”); Cyber Digital Forensics Response LLC (“Cyber Digital”); 1st All Investments, LLC (“1st All Investments”); Salon Place LLC (“Salon Place”); VPR Academy LLC (“VPR Academy”); 21111 Chagrin Investments LLC (“Chagrin Investments”); and 4350 Renaissance LLC (“4350 Renaissance”).

former employees.³ Belkin orchestrates and participates directly in the scheme's deceptive core. Belkin personally drafted the deceptive telemarketing scripts and directed the creation of fake consumer reviews. *See* Sections II.C, I.H, *infra*. Belkin is aware of the longstanding pattern of customer complaints regarding Defendants' business practices.⁴ Belkin has authority to control the Corporate Defendants, including through the hiring and firing of employees.⁵ Belkin is the signatory for the Corporate Defendants' known bank accounts and controls the corporate budget.⁶ Belkin resides in Ohio, where he established and continues to supervise Corporate Defendants' headquarters.⁷ Defendants also operate their scheme through offices and employees based in Mexico, Costa Rica, India, Ukraine, Russia, Poland, the Philippines, and Canada.⁸

At Belkin's direction, Corporate Defendants operate as a common enterprise, using a web of corporate entities, fictitious names, websites, and international offices to deceptively market and sell sextortion assistance services.⁹ By registering and operating dozens of different websites

See Smedley Decl. ¶ 41 & Table 7 (showing Belkin registered agent, ownership, or membership status with Corporate Defendants). Belkin's long-time associate and Chief Technology Officer of DFC, Viktor Sobiecki, controls Cyber Digital, but Stripe records show the business address as the same 4400 Renaissance address as DFC. Smedley Decl. Table 3 & n.2.

³ Raffile Decl. ¶ 27; *see also* Smedley Decl. ¶¶ 25-26, Exhibits J, K, L (employee interviews).

⁴ Dilworth Decl. ¶¶ 25, 29, 44-49, Ex. B, Ex. D at 39:17-40:21.

⁵ Tolok Decl. ¶¶ 3, 39; Smedley Decl. Ex. K at ¶ 2, Ex. L at ¶ 14.

⁶ Smedley Decl. ¶¶ 36-40, Tables 5-6; Dilworth Decl. ¶ 44, Ex. D at 16:6-10.

⁷ Tolok Decl. ¶¶ 5, 7; Smedley Decl. Ex. K at ¶ 2; Dilworth Decl. Ex. D at 12:15-16, 13:4-6.

⁸ Smedley Decl. Ex. K at ¶¶ 2-4 (former employee recalls Mexico, Costa Rica, Poland locations); Raffile Decl. ¶¶ 7, 46 (Ohio, Mexico, Costa Rica, India); Tolok Decl. ¶¶ 4-5 (Ukraine, Mexico, Ohio, Costa Rica, Philippines, India, Russia). Belkin works in the primary office location in Ohio, but frequently travels to Florida, Mexico and Costa Rica, where Defendants have or had additional office buildings or addresses. Smedley Decl. Ex. K at ¶¶ 2-4; Dilworth Decl. Ex. D at 34:11-15.

⁹ Belkin admitted to the Better Business Bureau ("BBB") that multiple entities "are doing business as Digital Forensics, and they all service clients [as] Digital Forensics" but "all [the clients] know is our DBA, which is Digital Forensics Corporation. That's all they know." *See* Dilworth Decl. Ex. D at 15:2-5, 33:14-22. In fact, Belkin acknowledges, "clients . . . don't know which company in essence serviced them. They all go to Digital Forensics." *Id.* at 30:9-15.

that re-route to one another, Corporate Defendants lure in thousands of unsuspecting consumers.¹⁰ For example, consumers who try to visit the websites onlineblackmail911.com or stopblackmail.org are automatically re-routed to one of Corporate Defendants' primary websites, blackmailhelpline.com.¹¹ Belkin and his associates often pay extra for a service that conceals the identity of the domain registrant.¹²

Corporate Defendants use an ever-evolving rotation of names and aliases to market and sell their sextortion assistance services. For example, the sextortion assistance service contracts provided to consumers use the name 1st All File Recovery d/b/a Digital Forensics Corp, or, more recently, 1st All File Recovery USA Inc., d/b/a Blackmail Helpline.¹³ Yet, after purchasing services, customers subsequently receive documents and correspondence from numerous other entities.¹⁴ It is nearly impossible to distinguish the various Corporate Defendants from one another due to their use of similar or identical names and fictitious names.¹⁵

1st All File Recovery, I & D Belkin, and 1st All Data Recovery do “exactly the same business” under the name Digital Forensics Corp, aka Defendant DFC. *See* Dilworth Decl. ¶ 44 & Ex. D at 14:14–15:12.

¹⁰ Smedley Decl. ¶ 46; Table 8; Dilworth Decl. Ex. D at 18:11–14 (10,000–15,000 clients per year).

¹¹ Smedley Decl. ¶ 53 & Table 9.

¹² Smedley Decl. ¶ 44.

¹³ Smedley Decl. Ex. G at 48; Boyer Decl. Ex. B.

¹⁴ Smedley Decl. Ex. E at 5 (Customer of Blackmailhelpline reporting “I have noticed that the company in the email they sent me is different name from the one on their google page that I originally found. Their second name is Cyber Security Corp and they have a different email address listed as info@cybersecuritycorp.com”); Boyer Decl. Ex. A (Blackmail Helpline customer receiving receipt from merchant “Data Recovery – OH”), Ex. C (email from cybersecuritycorp.com, enclosing DFC videos), & Ex. E (emails from cybersecuritycorp.com).

¹⁵ 1st All File Recovery, 1st All Data Recovery, and I & D Belkin all do business under the name “Digital Forensics” or a variation thereof, mirroring the actual DFC entity. Dilworth Decl. ¶ 44 & Ex. D at 14:14–15:12, 33:14–22; Smedley Decl. Table 2. Similarly, Remote Backup Corp does business as Digital Cyber Forensics Investigation, an effectively identical name to Corporate Defendant Digital Cyber Forensics Investigations LLC. Smedley Decl. ¶ 23, Table 2.

Adding to the confusion, the same employees work for multiple Corporate Defendants, as evidenced by consumer complaints against the various companies.¹⁶ Long-term DFC employees are also listed on corporate filings for Cyber Digital, Cyber Investigation, and Chagrin Investments.¹⁷ On corporate filings and bank records, all the Corporate Defendants list their corporate address as 4400 Renaissance Parkway, Suite 1, Warrensville Heights, Ohio 44128 or 3570 Warrensville Center Road, Suite 211, Shaker Heights, Ohio 44122.¹⁸

The Corporate Defendants commingle funds, routinely transferring large sums of money back and forth among one another.¹⁹ Defendants dissipate vast sums of money, often spending consumer funds soon after they are received.²⁰ Belkin has spent millions in corporate funds for the personal benefit of himself and his family members, including by purchasing a boat and jet ski, paying more than \$38 million toward his personal credit cards, and paying more than \$1.4 million toward credit cards in the name of his father.²¹

Defendants have a history of destroying evidence and threatening those who speak out. Defendants force customers and former employees to sign contracts with “confidentiality” and “non-disclosure” provisions, then threaten legal action not only against the signatories, but also those who “induce” the signatories to breach their contracts.²² Three of four former employees interviewed by FTC staff declined to sign declarations in this action, with two expressly citing

¹⁶ Smedley Decl. ¶ 12.

¹⁷ Smedley Decl. Table 1, Table 2 & n.1; Ex. H (incorporation records).

¹⁸ *See generally* Smedley Decl. Ex. M (Fifth Third and CF Bank records); *see also* Exhibit H (incorporation records).

¹⁹ Agarwal Decl. ¶¶ 15–17. Notably, Defendant DFC does not appear to have a bank account, despite serving as the namesake of the common enterprise. Smedley Decl. ¶ 35 n.3, ¶ 38 n.4. About 50% of consumer payments are funneled through 1st All Data Recovery. Agarwal Decl. ¶ 19.

²⁰ Agarwal Decl. ¶¶ 19–26; *see also* Smedley Decl. ¶ 40.

²¹ Agarwal Decl. ¶¶ 22, 24; Smedley Decl. ¶ 40 (jet ski and boat on P&L statements).

²² Raffile Decl. ¶¶ 7, 42 & Ex. D.

non-disclosure agreement obligations and fear of retaliation.²³ Likewise, FTC staff contacted more than eighty consumers who filed complaints against Defendants and fewer than fifteen responded.²⁴ Even fewer agreed to speak with FTC staff or sign a declaration, with several alluding to concerns of breaching a confidentiality agreement.²⁵

B. Sextortion Background

Sextortion is a rapidly growing national threat.²⁶ In a financial sextortion attack, the “sextortionist,” obtains nude or sexual images of the victim and threatens to publicize the images unless the victim pays the sextortionist.²⁷ Upon learning they are being blackmailed, victims of sextortion become panicked, fearing the personal and professional repercussions of their intimate

²³ Smedley Decl. ¶ 29; Exs. J ¶ 12, L ¶ 1 (interview notes with former employees referencing non-disclosure agreements); *see* Tolok Decl. (former employee declaration).

²⁴ Smedley Decl. ¶ 28.

²⁵ Smedley Decl. ¶ 28. Several other complainants expressed that they were not comfortable signing a declaration due to the highly personal nature of their experience. *See* Smedley Decl. ¶ 28. Thus, some evidentiary materials submitted herewith incorporate hearsay, including Investigator Smedley’s summary of her interviews with former employees and copies of consumer complaints submitted regarding Defendants. Courts routinely consider hearsay evidence when determining whether to grant a TRO or preliminary injunction. *See, e.g., Chefs’ Warehouse Midwest, LLC v. CSX Transp., Inc.*, No. 1:17-CV-555, 2017 WL 3872484, at *4 (S.D. Ohio Sept. 5, 2017); *see also Mullins v. City of New York*, 626 F.3d 47, 52 (2d Cir. 2010) (collecting circuit and district court cases).

²⁶ Coffren Decl. ¶¶ 5-10; *see also* FBI, “Sextortion: A Growing Threat Preying Upon Our Nation’s Teens,” *available at* <https://www.fbi.gov/contact-us/field-offices/sacramento/news/sextortion-a-growing-threat-preying-upon-our-nations-teens>.

²⁷ *See* FBI, “Financially Motivated Sextortion,” *available at* <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/sextortion/financially-motivated-sextortion>. While sextortion over sexual images is common, online scammers may use other means to extort or blackmail victims. For example, “romance scams” involving a fake online relationship may proceed to extortion. *See* FBI, “Romance Scams,” *available at* <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/romance-scams>.

photos or videos being posted online or sent to their friends and family.²⁸ Many victims of sextortion report feeling so distressed that they contemplate suicide.²⁹

Law enforcement agencies, like the Federal Bureau of Investigation (“FBI”), and non-profit organizations, like the National Center for Missing and Exploited Children (“NCMEC”), with expertise in sextortion cases, typically recommend that victims: (1) should not pay the sextortionist, and (2) should instead (a) block the sextortionist’s communications and (b) report the sextortionist to the authorities.³⁰ The FBI and NCMEC also recommend *against* paying for-profit companies for assistance with a sextortion attack.³¹ There are numerous non-profit support services and legal protections available to sextortion victims, free of charge. For example, in response to the escalating harms from non-consensual intimate image (“NCII”) abuse, Congress enacted the TAKE IT DOWN Act, which criminalizes the distribution of NCII and requires covered platforms to remove NCII within 48 hours of a victim’s request.³² Non-profits, like NCMEC, also offer extensive support and assistance to victims, including by offering mental health resources and assisting victims with reporting the attack to relevant authorities.³³

²⁸ Smedley Decl. ¶ 11.a & Ex. A.

²⁹ R. Liggett O’Malley & K. Smith, *Suicidal Ideation Among Male Victim-Survivors of Financial Sextortion*, 20 Victims & Offenders 1285 (2025); FBI, “The Financially Motivated Sextortion Threat,” *available at* <https://www.fbi.gov/news/stories/the-financially-motivated-sextortion-threat> (FBI aware of at least 20 suicides due to sextortion); Tolok Decl. ¶ 35; Coffren Decl. ¶ 8 (36 known suicides by teenage boys targeted for sextortion); Smedley Decl. ¶ 11.a & Ex. A.

³⁰ Coffren Decl. ¶¶ 12, 16, 21; FBI, “Sextortion,” *available at* <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/sextortion/sextortion> (hereinafter, “FBI Guidance”)

³¹ Coffren Decl. ¶¶ 12, 16, 21; FBI Guidance (“Victims of sextortion should never have to pay fees to receive assistance or to have their non-consensual images removed from online or in-app postings.”).

³² Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (“TAKE IT DOWN Act”), Pub. L. No. 119-12, § 146, 139 Stat. 55 (2025).

³³ Coffren Decl. ¶¶ 11, 14–20.

C. Defendants' Deceptive Marketing of Unnecessary Sextortion Services

Since at least 2020, Defendants have falsely advertised and sold their sextortion assistance services to thousands of consumers nationwide.³⁴ Approximately 90–95% of Defendants' business is sextortion assistance services,³⁵ and financial records show that consumers have paid Defendants at least \$60 million in the last three years.³⁶ Defendants spend millions of dollars on advertising, ensuring their advertisements are featured prominently on platforms like Google and YouTube.³⁷ Due to Defendants' aggressive online advertising, Defendants' websites and advertisements are often the first search results when a sextortion victim searches online for help.³⁸ Defendants operate multiple websites under different names that tout Defendants' ability to stop sextortion attacks.³⁹

³⁴ Smedley Decl. ¶¶ 7-11 (complaints), ¶ 28.d, Ex. R (USA Today article); Dilworth Decl. Ex. D at 18:11–14 (10,000 – 15,000 clients per year).

³⁵ Raffile Decl. ¶ 23; Smedley Decl. ¶ 26, Ex. K at ¶ 5 (DFC's sextortion services were largest seller, "exploded" during the Covid pandemic).

³⁶ Agarwal Decl. ¶ 14 & Table 3. FTC staff have not yet obtained records for all of Corporate Defendants' bank accounts, therefore this is likely an underestimate of funds obtained from consumers. *See* Agarwal Decl. n.2; *see also* Dilworth Decl. Ex. D at 35:3–9 (Belkin discussing "\$30 million plus per annum" earnings from DFC-related entities).

³⁷ Smedley Decl. ¶ 40 (P&L statements showing money spent on advertisements) ¶¶ 57-58 (Smedley captures of online ads, including Google search results & YouTube videos); Ex. A at 1 ("I was a victim of a sextortion scam. Being very stressed and scared I went to the first website to sign up for blackmail and sextortion care. It ended up being this company (Digital Forensics Corp.)"); Ex. A at 18 ("After I received the blackmail I immediately searched for experts on the subject. Digital Forensics was the first result on the list."); Raffile Decl. ¶ 5.

³⁸ Boyer Decl. ¶ 3; Smedley Decl. Ex. A at 18; ("I was a victim of blackmail and sextortion. I was scared beyond belief and experiencing severe anxiety and panic attacks following the event. I already have an anxiety condition. After I received the blackmail I immediately searched for experts on the subject. Digital Forensics was the first result on the list."); Ex. A at 21 ("I was [a] victim of online extortion and i was freaked out and called Digital Forensic Corp being the first group that popped up in a google search"); Ex. A at 13; Raffile Decl. ¶ 18–20 and Ex. A.

³⁹ Smedley Decl. ¶¶ 55-56 (Google searches) ¶ 13.f (BBB websites identified, including cyberblackmail911.com, securitybreach911.com, cybersecuritycorp.com); ¶ 52, Table 8 (domain names); Raffile Decl. ¶ 18

Defendants' advertisements weaponize victims' fears and lure victims away from legitimate support services.⁴⁰ For example, a victim searching on Google will see, at the top of the search results, an advertisement reading "The Police Can't Help You. We Can - Don't Wait - Act Now. Call."⁴¹ Upon visiting Defendants' websites, victims are advised that publicization of their explicit photos will "Destroy Your Family Life and Reputation," specifically by leading to divorce, "loss of parental rights," and getting fired.⁴² Defendants' websites reiterate that "the legal system and police won't help" with a sextortion attack, urging victims to seek assistance from Defendants right away.⁴³

Defendants' websites prompt victims to submit their contact information through an electronic form, with "Report Sextortion" in bold letters at the top. Instead of providing free advice, like many consumers expect from a "helpline," Defendants rush to make a sale through a coercive telemarketing call.⁴⁴ During these phone calls, Defendants follow a deceptive script

⁴⁰ Smedley Decl. Ex. B at 3 (consumer complaints) ("[T]alked to Digital forensics corp and thought they could help but they really just tried to make me more worried about what the scammer would do with my picture. I ended up paying them some money to take over my accounts and deal with the scammer. After time to read up on what I should do, I deactivated all my accounts and blocked the scammer, and will be trying to get some money refunded from DFC."); Ex. B at 22 ("I spoke with a [DFC] representative during a exploitation text from a scammer. I was not certain about using the service but he convinced me that I was doing the right thing. . . . I foolishly gave in. . . . Two weeks later on the local news they were talking about the subject and recommended to just block the [scammer]. The ethics behind Digital forensics is very questionable.")

⁴¹ Raffile Decl. Ex. A, at 1.

⁴² Smedley Decl. ¶ 67, Ex. Q at 2 (website screenshot of BlackmailHelpline.com).

⁴³ Smedley Decl. ¶ 67, Ex. Q at 6; *see also* Raffile Decl., Ex. A ("The Police Can't Help You. We Can - Don't Wait - Act Now. Call.").

⁴⁴ *See* Smedley Decl. Ex. B at 15 ("Like many vulnerable people that reach out to this company. I just wanted to report the incident. But they reached back out and convinced me that I was in danger of a severe threat, and that I was dealing with professionals, and that I needed to sign up for their services immediately or I was at risk for worse")

drafted entirely by Belkin.⁴⁵ Defendants' telemarketers are required to mention multiple "pain points" that target the victim's fears and vulnerabilities.⁴⁶ For example, Defendants tell servicemembers that publicization of their explicit images can result in a dishonorable discharge.⁴⁷ Similarly, Defendants tell victims that are going through a divorce that sextortion could result in losing child custody.⁴⁸ Defendants also routinely tell victims that the sextortionist will digitally modify their explicit images to make it appear the victim engaged in sexual activities with a minor, leading the victim to believe they may face criminal punishment.⁴⁹ As

⁴⁵ Raffile Decl. ¶ 27 and Ex. B; Smedley Decl. Ex. K at ¶ 7 ("100% of script approvals" from Belkin), L at ¶ 4 ("Dmitry [Belkin] did all of the scripts").

⁴⁶ Raffile Decl. ¶¶ 25–27 and Ex. B at 22–26; Smedley Decl. Ex. L at ¶ 4. Former employees report that if they deviated from the telemarketing script, they were punished, including by having their compensation reduced. Smedley Decl. Ex. L at ¶ 4; Raffile Decl. ¶ 25; *see also* Smedley Decl. Ex. A at 21 (consumer complaints) ("[I] was [a] victim of online extortion and i was freaked out and called Digital Forensic Corp being the first group that popped up in a google search and requested help[.] [T]he 1st phone call was basically me being scared to death as the[ir] employee was telling me that all these thing would happen to me if [I] didn't buy the[ir] service."); Ex. A at 18 ("They made up a lot of things that I believed to be true. That the[sextortionist was] going to track me down and this could ruin my relationships and everything. I would lose my job and the blackmailers would not stop. This scared me greatly so I paid them asap to prevent any of this from happening.")

⁴⁷ Raffile Decl. Ex. B at 23.

⁴⁸ Raffile Decl. Ex. B at 25.

⁴⁹ Raffile Decl. Ex. B at 13 ("They will often manipulate the pictures/videos to appear like you were chatting with someone who is underage, or trying to meet up with a minor"), Ex. B at 23 ("I've seen these situations ruin people's retirement all from the accusations of being a child predator."); Smedley Decl. ¶¶ 25–27, Ex. I at 15:6–15 (undercover recorded call, "[sextortionists] even go as far as fabricating content to make it seem that their victims are trying to meet up with minors"); Ex. B at 20; ("[T]he [DFC] agent also capitalized on my nervous state of mind by explaining how the scammer could take my photos and photoshop them with minors and create the image of me as pedophile to destroy my career. He (the agent) hyped his brand's image as absolutely necessary to end the sextortion and to keep my career reputation intact."); Ex. B at 1 ("I googled (someone's trying to expose my picture), and digital forensics emerged. They started to use scare tactics on me, saying if you don't use the[ir] services, They will post you with a minor; this could ruin your life."); Ex. B at 5 ("I came across a group called Digital Forensics Corp, and contacted them. . . . and they came at me with scare tactics to lure me into purchasing their product. Saying that the photo can be manipulated and photoshopped next to a minor, and that it's hard to erase that title from your name even if I'm proven innocent."); Ex. B at 25; *see also* Boyer Decl. ¶ 4.

described in one customer complaint: “the representative used high-pressure tactics that caused me significant fear and stress, including statements implying that if I did not sign immediately, my situation would worsen.”⁵⁰ According to a former employee, Defendants’ strategy is “to scare people so that they would pay more money.”⁵¹

After informing victims their situation is “severe,” Defendants pressure victims to purchase “Phase 1” sextortion assistance services. Defendants claim Phase 1 is so effective at getting sextortionists to “walk away” that customers rarely require additional Phase 2 services.⁵²

Defendants charge \$1,499 to \$20,000 for Phase 1 sextortion assistance services.⁵³ If a victim agrees to purchase Phase 1, Defendants obtain payment information—including debit and credit card numbers—during the sales call, often before sending a copy of the service contract.⁵⁴ Consumers report that they purchase these services based on the explicit and implied representations that Defendants’ services will stop further sextortion.⁵⁵

D. Defendants Fail to Perform Promised Phase 1 Services

Defendants expressly represent during interstate telemarketing calls that Phase 1 includes Defendants: (1) taking over communications with the sextortionist, (2) tracing the sextortionist’s location through a “tracking campaign,” (3) producing a detailed investigative report, (4) sending a cease-and-desist letter to the sextortionist, (5) reporting the sextortionist to law enforcement,

⁵⁰ Smedley Decl. Ex. A at 9; *see also* Ex. A at 7 (“I was blackmailed and contact[ed] them online. After being told I was in serious trouble I signed up for their 3 day service.”).

⁵¹ Tolok Decl. ¶ 27.

⁵² Smedley Decl. Ex. I at 24:17-22 (undercover call transcript) *see also* Ex. Q at 7 (“success rate” of more than “90 percent”).

⁵³ Smedley Decl. ¶ 11.c (prices quoted to consumers); Ex. I at 29:18-20 (telemarketer offering \$1,499 service), 30:20-22 (\$2,999 service), 31:1-2 (\$4,999 service); 31:114-16 (\$7,200 service); 32:3-4 (\$20,000 “VIP” service).

⁵⁴ Lydick Decl. ¶ 5; Boyer Decl. ¶ 6; Smedley Decl. Ex. I at 37:2-5 (telemarketer offering \$1,500 service by credit or debit card); Raffile Decl. Ex. B at 31–32.

⁵⁵ Smedley Decl. Ex. C (exemplary complaints regarding failure to stop attacks).

and (6) stopping the sextortion attack.⁵⁶ Defendants routinely do not deliver these services or stop sextortion attacks.

A key aspect of the Phase 1 service is Defendants' promise to log in to the victim's social media or other accounts to continue communicating with the sextortionist, which is supposedly necessary to investigate and track the sextortionist's location. For this reason, Defendants expressly require customers to maintain or reinitiate communications with the blackmailer—falsely claiming that blocking and ignoring the sextortionist is “the last thing you want to do”⁵⁷—in direct contradiction with FBI and NCMEC guidance to block sextortionists.⁵⁸ Defendants' false claims induced victims to pay for their services, then, in numerous instances, Defendants logged into victims' accounts and simply blocked the sextortionist without ever communicating.⁵⁹ To conceal this, Defendants (1) prohibit victims from logging into their own accounts,⁶⁰ (2) delete the original chat logs from the victims' accounts, and (3) create fake chat

⁵⁶ Raffile Decl. Ex. B at 7 (“we assume communication acting as you, we track the criminals, we confront the criminals, we get them to leave you alone” and “We have an extremely high success rate in preventing private and personal materials from being posted or shared”); Smedley Decl. Ex. I (undercover call transcript); Exs. A-F (complaints from multiple states).

⁵⁷ Smedley Decl. Ex. I at 5:13-22 (telemarketer telling FTC investigator that “the last thing you want to do” is block, delete, or ignore a sextortionist); Boyer Decl. Ex. C, at 1 (“Please stay in communication with the suspect per your case manager's instructions.”); Raffile Decl. Ex. B at 10–11 (“If you aren't in contact with the suspect we would not be able to help . . . If they think you are ignoring them they could start releasing your information to get your attention. Can you get back in contact with the suspect?” and “ignoring them is not an option either. This will piss them off and they will release the pictures/videos” and “I've talked to other victims that have tried this tactic and it's backfired almost immediately”).

⁵⁸ FBI Guidance; Coffren Decl. ¶ 12; Smedley Decl. ¶ 25-27 (undercover call); Raffile Decl. Ex. A.

⁵⁹ Smedley Decl. Ex. L at ¶ 6; Ex. C at 5 (“I decided to log into my accounts on the second day they took over, and all I saw was that the blackmailers were blocked.”); Ex. A at 7.

⁶⁰ Raffile Decl. Ex. B at 17 (“when the analyst is in control of your accounts it is vital that you stay out of those accounts . . . Logging into your accounts . . . will put your investigation at risk.”); Tolok Decl. ¶ 13.

conversations that are screenshotted and pasted into the “Phase 1 report” summarizing the investigation, which is provided to the customer.⁶¹

The “tracking” component is equally fabricated. Multiple former employees report that Defendants do not trace sextortionists’ locations and instead insert made-up GPS coordinates into Phase 1 reports.⁶² Despite promising to report the sextortionist to law enforcement in Phase 1, Defendants pull a bait-and-switch, insisting that they will only contact law enforcement if the victim purchases Phase 2 services.⁶³

E. Defendants Upsell Phase 2 Services and Fail to Deliver Them

Despite claiming that Phase 2 services are “rarely” required, Defendants, in fact, pressure every customer to purchase Phase 2 for thousands of dollars.⁶⁴ During high-pressure sales calls, Defendants use the made-up details from their Phase 1 “investigation” to coerce victims into paying for “extra protection” in Phase 2, oftentimes falsely claiming that the sextortionist is unusually “dangerous” or “vicious.”⁶⁵ Defendants promise that in Phase 2 they will (1) contact law enforcement to report the sextortionist’s crimes and (2) monitor the victim’s accounts and the Internet in case the sextortionist renews the attack or releases the victim’s explicit material.⁶⁶

⁶¹ Tolok Decl. ¶¶ 19–20; Smedley Decl. Ex. L at ¶ 6; By deleting the chat logs, Defendants ensure victims have no way to determine whether Defendants actually communicated with the sextortionist or whether the screenshots shown in the Phase 1 report are fabricated. *See* Tolok Decl. ¶ 19.

⁶² Smedley Decl. Ex. L at ¶ 7-8; Tolok Decl. ¶¶ 16–17, 22–23.

⁶³ Smedley Decl. Ex. C at 26 (“The company misrepresented the service as a full solution (investigation + legal action) for \$1,499, but buried in the contract that “phase 2” costs thousands more. I was also threatened with legal action if I contacted BBB, the FTC, or my state Attorney General.”); *see also* Ex. C at 12.

⁶⁴ Tolok Decl. ¶¶ 24–26 (“DFC instructed us to recommend Phase 2 services to every client, even though Phase 2 services were not needed.”); Lydick Decl. ¶¶ 10–11; Smedley Decl. Ex. K at ¶ 11.

⁶⁵ Smedley Decl. Ex. D at 5, 19, 22.

⁶⁶ Tolok Decl. ¶ 28; Raffile Decl. ¶ 36.

After extracting even more money from victims, Defendants yet again do not perform the promised tasks.

Defendants frequently do not attempt to contact law enforcement; when they do, the letters and emails are often returned undelivered and Defendants take no further action.⁶⁷ Multiple former employees do not recall any instance in which DFC worked with law enforcement to secure the arrest of a sextortionist.⁶⁸ Likewise, Defendants’ “monitoring” is a farce. Defendants either conduct zero monitoring or use ineffective, low-effort methods like setting a Google Alert for the victim’s name—which would not detect a renewed sextortion attack or private release of the victim’s explicit images.⁶⁹

Unsurprisingly, Defendants often fail to stop sextortion attacks. Many customers report that their sextortionist continued contacting them and multiple customers had their explicit

⁶⁷ Tolok Decl. ¶¶ 29-31; Raffile Decl. ¶ 31–33.

⁶⁸ Raffile Decl. ¶ 34; Tolok Decl. ¶¶ 28, 32.

⁶⁹ Tolok Decl. ¶¶ 29–30; Raffile Decl. ¶ 36; Smedley Decl. Ex. L at ¶ 10 (“account monitoring wasn’t happening”); Ex. D at 25 (“I started searching for companies and digital forensics came up. When I spoke to them they mentioned they had over a 90% success rate in stopping the extortionist. . . . They also said if the person did send [my photos], they would be alerted and it be taken down in seconds. . . . I paid an extraordinary amount of money for them to take over communications with this individual, and in less than one hour after them taking over communications, the individual began leaking the information. I called the analyst immediately asking what is happening, he had no idea this occurred. I had to send him screenshots of all the instances, as he could not find these posts. All he did was ask which accounts these were and . . . and literally the only thing they did was request to block the account. . . . I would have been better off dealing with this myself.”).

images publicized by the sextortionist after they hired Defendants.⁷⁰ At least 10 of Defendants' former employees have independently described the sextortion assistance services as a "scam."⁷¹

F. Defendants Do Not Honor Their Refund Policy

Defendants do not honor the express terms of their refund policy. Defendants' contracts provide for a partial refund if requested within 3 days.⁷² In practice, Defendants routinely delay responding until after the refund window expires.⁷³ Numerous customers have reported that Defendants rejected or ignored their refund requests entirely.⁷⁴

G. Defendants Ignore and Suppress Complaints

Consumers have complained about Defendants' fraudulent business practices for the better part of decade, but instead of ceasing their misconduct, Defendants respond by selling new useless services under different aliases.

⁷⁰ Tolok Decl. ¶¶ 33–36 (“I remember multiple clients whose photos and videos were released publicly by the sextortionist, even though DFC was hired to work on the case. . . . I remember that DFC’s sales script said DFC had a 90% success rate. I believe that the 90% success rate is a made up number.”); Smedley Decl. L at ¶ 3; Ex. D at 25 (“I paid an extraordinary amount of money for them to take over communications with this individual, and in less than one hour after them taking over communications, the individual began leaking the information.”) Ex. C at 11 (“This company says they will take care of the extortionist and have the know how and proprietary software and will stop the bad guys. 90% success rate. \$3000 got me nothing. Scammers are back after one week. Their services failed.”); Lydick Decl. ¶¶ 8, 12.

⁷¹ Raffile Decl. ¶¶ 8, 37; Smedley Decl. Ex. L at ¶ 3 (“Everything they sell is a scam”) Tolok Decl. ¶ 29.

⁷² Smedley Decl. ¶ 11.f; Ex. E at 5 (“although their contact [sic] states that I have 3 days to get refund and they said I could not.”), 19 (DFC delayed meeting until third day to avoid refund period); Ex. G at 36-37 (DFC contract with “Non-payment provision” giving 3-day window for payment disputes).

⁷³ Smedley Decl. Ex. E at 19 (“They made me wait 3 days before I even knew what I was really paying for. I tried to contact my ‘case manager’ on day 2 but he made me wait until the afternoon of day 3 to discuss with me”), 30 (“my mom wants a full refund because she did not receive any of the services that they are trying to charge her for”).

⁷⁴ Smedley Decl. Ex. E at 27 (“they had me sign a document saying that they were going to refund me \$2000 and the refund NEVER occurred.”), Ex. E at 5; Boyer Decl. ¶ 10.

For example, in 2018 the Better Business Bureau (“BBB”) identified a pattern of complaints alleging Defendants misrepresented their “Phase 1” and “Phase 2” services, but in relation to a “data recovery” scheme, where Defendants claimed that additional evidence, emails, photos, or other data could be recovered from electronic devices if the consumer paid more money for Phase 2.⁷⁵ The BBB notified Defendants of the pattern of complaints and Defendants blamed it on “mismanaged and poorly trained employees.”⁷⁶ In 2020, after Belkin realized the potential to profit from the growing number of sextortion cases, Defendants increasingly pushed their sextortion services and by 2021, the BBB had identified a similar pattern of complaints regarding those services.⁷⁷

In just the past three years, more than 500 consumers have filed complaints against Defendants with the BBB, the FTC, and state Attorneys General.⁷⁸ Consumers also complain directly to Defendants—in the year 2024 alone, 572 customers submitted negative feedback in response to Defendants’ “satisfaction survey.”⁷⁹ These complaints overwhelmingly report that Defendants use fear-mongering tactics and false representations to sell their sextortion assistance services, then do not fulfill their promises and refuse to provide refunds.⁸⁰ Many consumers

⁷⁵ Dilworth Decl. ¶ 19; *see also* Smedley Decl. Ex. F at 3 (“On May 9, 2024 I paid digital forensics \$749 to try and extract information from an iPad I sent them. Roughly a month later they emailed me a Phase One report In the report they identified a chat I wanted to see. They promised in writing (email) that if I paid \$3200 they would immediately give me a printout of that conversation On June 25, 2024 I paid the money and they began dodging my calls.”)

⁷⁶ Dilworth Decl. ¶ 20.

⁷⁷ Raffile Decl. ¶ 23; Smedley Decl. Ex. K at ¶¶ 13-14; Dilworth Decl. ¶¶ 12-13, 21, 30 & Ex. A.

⁷⁸ Smedley Decl. ¶ 7.

⁷⁹ Raffile Decl. ¶ 43 & Ex. C.

⁸⁰ Smedley Decl. Ex. D at 1 (“I expected 14000 for phase 1 and phase 2 to be somewhat better as it was their 2nd or 3rd highest service. However, I did more for myself with free government services than they did.”); Dilworth Decl. ¶ 24.

describe feeling re-victimized by Defendants after they had already endured a sextortion attack.⁸¹

While the majority of complaints over the past three years were filed against DFC—the entity name most commonly used to market the sextortion services—the most recent complaints are piling up against “Blackmail Helpline,” an unregistered fictitious name for 1st All File Recovery.⁸² This recent shift indicates Corporate Defendants have begun marketing the same sextortion services under a new name, likely to evade DFC’s negative online reputation.⁸³

Defendants continue to ignore and aggressively suppress negative feedback. Defendants refuse to refund customers unless they agree to sign a non-disparagement clause, that not only prohibits any future negative reviews, but requires the customer to remove any existing negative reviews.⁸⁴ According to one former employee, Defendants assigned him to monitor negative online reviews and attempt to match the details with a particular client, then contact the customer and pressure them to remove their negative review, claiming they were breaching a confidentiality provision in the sales contract.⁸⁵ According to another former employee,

⁸¹ Smedley Decl. Ex. B at 34 (“These people will fearmonger you into buying their services. DO NOT TRUST THESE PEOPLE. They are worse than the actual criminals.”); Ex. B at 8 (“They may be worse than the actual criminals. I purchased these services on 04/22/2023. Digital Forensics will take advantage of you in your worst possible state of mind. I feel taken advantage of by these people. Please reconsider before using them. They are definitely more concerned about the money, same as the crooks.”); Ex. B at 29 (“They are trying to fear me into paying for the full report. Almost worse than the actual blackmailers.”)

⁸² Smedley Decl. ¶ 10; Boyer Decl. & Ex. B. The service contracts are essentially identical to the sextortion assistance contracts used by 1st All File Recovery d/b/a Digital Forensics Corp.

⁸³ See Smedley Decl. Ex. E at 23 (“I quickly began to realize that they were a scam when I noticed that they’re not BBB accredited, their address is at a sketchy location, and many customers’ reviews mentioned that the organization makes the problem worse, not better.”); Dilworth Decl. ¶ 44 & Ex. A.

⁸⁴ Smedley Decl. Ex. J at ¶¶ 9-10 (former DFC employee could only offer refunds if customers signed a release); Ex. E (exemplary complaints on refund issues and waivers); Dilworth Decl. ¶¶ 28-29 & Exhibit B.

⁸⁵ Raffile Decl. ¶ 42; see also Tolok ¶ 37 (“I also heard that DFC would try to delete negative reviews that clients posted online.”).

Defendants route dissatisfied customers to a fake BBB website controlled by Defendants, so negative reviews are sent directly to Defendants rather than the real BBB.⁸⁶

H. Defendants Disseminate Fake Positive Reviews

In addition to suppressing negative reviews, Defendants deceive consumers by creating and disseminating fake positive reviews, to create the false impression Defendants have many happy customers.

Beginning in 2024, the BBB detected a suspicious pattern of activity, wherein a negative review submitted regarding DFC would often be followed by an influx of positive reviews about the company.⁸⁷ The BBB could not verify at least 234 five-star reviews submitted for DFC and refused to publish them, citing “significant concerns” about authenticity.⁸⁸ The BBB notified Belkin of the issue via letter and in a subsequent telephone call, and Belkin repeatedly insisted that the reviews should be published regardless.⁸⁹

Defendants’ former employees confirm two organized fake review schemes.⁹⁰ First, Belkin instructed employees how to submit fake reviews to Google that would be published, not flagged as inauthentic.⁹¹ Belkin advised employees to mail packets of paper, with “Digital Forensics Corporation” in on the first page, to random U.S. cities.⁹² Next, the employees had to hire Uber drivers—who had never used Defendants’ services—to retrieve the paperwork, drive to

⁸⁶ Smedley Decl. Ex. L at ¶ 13 (“DFC would send fake BBB links to ‘unhappy’ customers. If the unhappy customer tried to submit a negative review using the link from DFC, their negative review went to DFC and not the BBB.”).

⁸⁷ Dilworth Decl. ¶¶ 31, 47.

⁸⁸ Dilworth Decl. ¶ 38. The BBB also declined to publish an additional 44 four-star reviews for the same reason. *Id.* ¶ 39.

⁸⁹ Dilworth Decl. ¶¶ 41–48.

⁹⁰ A third former employee also recalls more generally that DFC’s IT Department created “fake positive customer reviews that DFC would use to advertise.” Tolok Decl. ¶ 37.

⁹¹ Smedley Decl. Ex. L at ¶ 12.

⁹² Smedley Decl. Ex. L at ¶ 12.

an unoccupied office building nearby, take a photo in front of the building while holding up the paperwork, and post a positive Google review regarding DFC's services, with the photo attached.⁹³ According to Belkin, submitting a review with an attached photo taken in the same location would circumvent Google's filters, allowing the fake reviews to be posted.⁹⁴

Second, DFC employees in India are responsible for posting fake positive reviews on ResellerRatings.com.⁹⁵ These fake positive reviews are the basis for the claim on DFC's website that it has been rated "5 out of 5 stars based on 3542 user reviews."⁹⁶

Defendants were also banned from posting on a popular online sextortion forum after site administrators determined that numerous posts containing positive feedback for DFC were actually posted by Defendants using various aliases.⁹⁷

I. Defendants Abuse and Manipulate the Judicial Process

Defendants have repeatedly shown that they have little respect for the judicial process. In response to a subpoena issued by a law enforcement agency, Defendants seemingly submitted falsified business records, at minimum, falsified telemarketing scripts and employee records.⁹⁸ Notably, the telemarketing script provided to the law enforcement agency did not contain any reference to the scare tactics that are most commonly reported by customers, and which were captured on an undercover call conducted by FTC Investigator Tiffany Smedley.⁹⁹ A second copy of the telemarketing script, that FTC declarant Paul Raffile received directly from a DFC

⁹³ Smedley Decl. Ex. L at ¶ 12.

⁹⁴ Smedley Decl. Ex. L at ¶ 12.

⁹⁵ Raffile Decl. ¶¶ 46-47.

⁹⁶ Raffile Decl. ¶ 46; Smedley Decl. ¶¶ 71-73, Ex. T.

⁹⁷ Raffile Decl. ¶ 45; Smedley Decl. ¶ 69-70, Ex. S.

⁹⁸ Raffile Decl. ¶ 50; Smedley Decl. ¶ 19 (discuss script versions don't match, causing concerns documents were falsified *prior* to hearing from Raffile's source).

⁹⁹ Smedley Decl. ¶¶ 25-27.

employee, contains numerous examples of the scare tactics commonly observed during Defendants' telemarketing calls.¹⁰⁰ This significant discrepancy between the two versions of the scripts strongly indicates that Defendants provided a falsified version of the telemarketing script that removed some of the most egregious language.¹⁰¹ Moreover, a former employee came forward and reported that Defendants did, in fact, provide falsified evidence to the same law enforcement agency.¹⁰²

This is not the first time Defendants have been accused of fabricating evidence or disregarding court rules. In 2025, a former employee alleged, with the support of an expert report, that 1st All File Recovery manufactured fake digital evidence to support its lawsuit accusing the former employee of misappropriating trade secrets.¹⁰³ The former employee further alleged that 1st All File Recovery spoliated evidence to cover its tracks.¹⁰⁴

III. ARGUMENT

This Court should issue an *ex parte* TRO enjoining Defendants' illegal practices and imposing other relief. The Court has the authority to issue the *ex parte* TRO, the FTC meets the standard for preliminary injunctive relief, and the scope of the proposed relief, described below, is necessary and appropriate.

A. The Court Has the Authority to Grant the Requested Relief

Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), authorizes the Court to enjoin practices that violate laws enforced by the FTC, including by granting temporary, preliminary and permanent injunctions. "[T]his broad grant of equitable power also gives courts 'the power to

¹⁰⁰ Smedley Decl. ¶ 20; *see also* Raffile Decl. Ex. B.

¹⁰¹ Smedley Decl. ¶ 20.

¹⁰² Raffile Decl. ¶ 50.

¹⁰³ Snell Rule 65 Decl. ¶ 14.

¹⁰⁴ Snell Rule 65 Decl. ¶ 14.

invoke ancillary equitable relief.” *FTC v. 6253547 Canada, Inc.*, No. 1:09-CV-1211, 2009 WL 10714993, at *2 (N.D. Ohio June 2, 2009) (quoting *FTC v. Amy Travel Serv.*, 875 F.2d 564, 571 (7th Cir. 1989)). “Thus, in addition to stopping the illegal conduct, a court may grant whatever additional relief is needed to preserve the effectiveness of the ultimate relief sought, which may include an order freezing assets[.]” *FTC v. Foreclosure Sols., LLC.*, No. 1:08 CV 1075, 2008 WL 11380125, at *6 (N.D. Ohio Nov. 21, 2008).

Section 19(b) of the FTC Act, 15 U.S.C. § 57b(b), separately authorizes courts to grant “such relief as the court finds necessary to redress injury to consumers” for violations of the TSR, Section 521 of the GLB Act, and the Reviews and Testimonials Rule, including the rescission or reformation of contracts, refund of money, and return of property. 15 U.S.C. § 57b(b).

B. The FTC Meets the Standard for Preliminary Injunctive Relief

In determining whether to grant a preliminary injunction, including a temporary restraining order, district courts within the Sixth Circuit weigh: (1) the likelihood of success on the merits, (2) irreparable injury, (3) the balance of equities, and (4) the public interest. *EOG Res., Inc. v. Lucky Land Mgmt., LLC*, 134 F.4th 868, 874 (6th Cir. 2025); *see also E.V. v. Raycraft*, No. 4:25-CV-2069, 2025 WL 2938594, at *5 (N.D. Ohio Oct. 16, 2025).¹⁰⁵ The FTC meets all four factors.

¹⁰⁵ Many courts relax the four-part standard in FTC cases, requiring only a showing of likelihood of success on the merits and a balance of the equities. *See, e.g., FTC v. Butterworth Health Corp.*, 121 F.3d 708 (Table), 1997 WL 420543, at *1 (6th Cir. July 8, 1997) (per curiam) (“The FTC need not prove irreparable harm to obtain a preliminary injunction under § 13(b).”); *Foreclosure Sols.*, 2008 WL 11380125, at *5; *6253547 Canada*, 2009 WL 10714993, at *2–3.

1. The FTC Is Likely to Succeed on the Merits

“In order to establish a likelihood of success on the merits of a claim, a plaintiff must show more than a mere possibility of success.” *Six Clinics Holding Corp., II v. Cafcomp Systems, Inc.*, 119 F.3d 393, 402 (6th Cir. 1997). The FTC has presented significant evidence, including sworn declarations from an FTC Investigator, an FTC forensic accountant, Defendants’ customers, and a former DFC employee, showing that the FTC has a strong likelihood of success on the merits of its claims Defendants violated Section 5 of the FTC Act, the TSR, Section 521 of the GLB Act, and the Reviews & Testimonials Rule.

a) *Defendants Make False or Misleading Representations to Market
Their Sextortion Services that Violate the FTC Act, TSR, and the GLB
Act*

Section 5 of the FTC Act prohibits material misrepresentations or omissions that would likely mislead consumers acting reasonably under the circumstances. *See FTC v. Foreclosure Sols., LLC*, No. 1:08 CV 1075, 2008 WL 11380125, at *5 (N.D. Ohio Nov. 21, 2008); 15 U.S.C. § 45(a). “A representation is material if it is likely to affect a consumer's decision to buy a product or service.” *FTC v. E.M.A. Nationwide, Inc.*, 767 F.3d 611, 631 (6th Cir. 2014) (citing *FTC v. Int'l Computer Concepts, Inc.*, 1995 WL 767810, at *2 (N.D. Ohio Oct. 24, 1995)). “Express claims are presumed to be material[.]” *FTC v. Int'l Computer Concepts, Inc.*, 1994 WL 730144, at *12 (N.D. Ohio Oct. 24, 1994). Consumer reliance on express claims is also presumed reasonable, because “[i]t is reasonable to interpret express statements as intending to say exactly what they say.” *Int'l Computer Concepts*, 1994 WL 730144, at *12 (citing *Thompson Medical Co.*, 104 F.T.C. 648, 788 (1984), *aff'd on other grounds* [1986–1 Trade Cases ¶ 67,103], 791 F.2d 189 (D.C. Cir. 1986), *cert. denied*, 479 U.S. 1086 (1986)).

The FTC need not establish that a particular consumer relied on and was injured by Defendants' misrepresentations. *E.M.A. Nationwide, Inc.*, 767 F.3d at 631 n.12. Instead, “[t]o raise a presumption of reliance, the FTC need only show (1) the business entity made material misrepresentations likely to deceive consumers, (2) those misrepresentations were widely disseminated, and (3) consumers purchased the entity's products.” *Id.* (quoting *FTC v. Freecom Commc'ns, Inc.*, 401 F.3d 1192, 1205 (10th Cir. 2005)). Likewise, it is not necessary to demonstrate that every consumer was harmed by a scheme.¹⁰⁶ *Amy Travel Service*, 875 F.2d at 572.

Similarly, Section 310.3(a)(2)(iii) of the TSR prohibits sellers and telemarketers¹⁰⁷ from “misrepresenting, directly or by implication, any material aspect of the performance, efficacy, nature, or central characteristics of goods or services that are the subject of a sales offer.” 16 C.F.R. §§ 310.3(a)(2)(iii). Moreover, Section 310.3(a)(4) prohibits sellers and telemarketers from making any false or misleading statements to induce a person to pay for goods or services. 16 C.F.R. § 310.3(a)(4).

Further, Section 521(a)(2) of the GLB Act bars the use of false or fraudulent statements to acquire a consumer’s banking information. Specifically, the act prohibits “any person” from “obtain[ing] or attempt[ing] to obtain . . . customer information of a financial institution relating to another person . . . by making a false, fictitious, or fraudulent statement or representation to a customer of a financial institution.” 15 U.S.C. § 6821(a)(2). “[C]ustomer information of a

¹⁰⁶ There is no intent element; the FTC need not prove that Defendants intended to deceive consumers. *E.M.A. Nationwide, Inc.*, 767 F.3d at 631 (citations omitted).

¹⁰⁷ “Telemarketing” is a “plan, program, or campaign . . . conducted to induce the purchase of goods or services . . . which involves more than one interstate telephone call.” 16 C.F.R. § 310.2(ii).

financial institution” refers to “information maintained by or for a financial institution which is derived from the relationship between the financial institution” and its customer that is “identified with the customer.”¹⁰⁸ 15 U.S.C. § 6827(2).

*i. Defendants Make Express Representations Regarding Their
Sextortion Assistance Services and Positive Customer Reviews*

Here, Defendants use numerous false and misleading representations to sell their sextortion assistance services to consumers. Defendants’ representations are widely disseminated—they are reflected on Defendants’ dozens of websites and made during the tens of thousands of telemarketing calls Defendants place per year.¹⁰⁹ Through the use of these false statements, Defendants attempt to obtain and do obtain consumers’ financial information.

As described in Sections II.C-D, Defendants routinely market and sell their sextortion assistance services through interstate telemarketing calls. During these telemarketing calls, Defendants represent to consumers that Defendants’ services will put a stop to the ongoing sextortion attack.

Defendants expressly represent during interstate telemarketing calls that the Phase 1 service includes: Defendants taking over communications with the sextortionist, Defendants conducting a tracking campaign to determine the sextortionist’s identity and location, Defendants providing the customer with a report containing truthful information collected about the sextortionist, and Defendants reporting the sextortionist to law enforcement. Thereafter, on subsequent interstate telemarketing calls, Defendants expressly represent that Phase 2 services

¹⁰⁸ A “customer” of a financial institution is “any person” or their authorized representative “to whom the financial institution provides a product or service.” 15 U.S.C. § 6827(1).

¹⁰⁹ Defendants state that they service approximately 10,000 – 15,000 customers per year, Dilworth Decl. Ex. B at 18:11-14, indicating Defendants make the express representations reflected in the telemarketing script to at least that many consumers each year.

include Defendants reporting the sextortionist to law enforcement and Defendants “monitoring” to detect and intervene in any renewed sextortion attack. *See* Section II.E.

Pursuant to the service contracts for Phase 1 and 2, Defendants expressly represent that consumers will receive a partial refund if it is requested within three days of signing the contract. Defendants also expressly represent, on their websites and other Internet platforms, that Defendants’ customers are publishing positive or five-star reviews regarding Defendants’ services. *See* Section II.H. For example, on DFC’s website, DFC claims to be rated “5 out of 5 stars rating based on 3,542 customer reviews.”

Defendants’ claims were expressly made, therefore they are presumed material. *See Int’l Computer Concepts*, 1994 WL 730144, at *12. Moreover, consumers confirm that Defendants’ representations influenced their purchase decisions. For example, consumers report that they purchased Phase 1 believing it would include law enforcement action. *See* Section I.D. Consumers also describe purchasing Defendants’ services based upon the representation the service would stop the sextortion attack.¹¹⁰ *See* Section II.C.

ii. Defendants’ Express Representations Are False

Defendants’ express representations were, in numerous instances, false. Critically, many consumers complain that Defendants did not successfully stop the sextortion attack. Many consumers report that, even after hiring Defendants, the sextortionist continued to threaten them and subsequently released their intimate images.

¹¹⁰ *See also* Smedley Decl. Ex. D at 16 (“If [DFC] would’ve told me that that was the criteria for needing phase 2, I wouldn’t have even done phase one.”). “[I]f consumers are likely to have chosen differently but for the deception, then a misrepresentation is material.” *Foreclosure Sols.*, 2008 WL 11380125, at *5 (citing *In re Southwest Sunites, Inc.*, 105 F.T.C. 7, 149 (1985), *aff’d* 785 F.2d 1431 (9th Cir. 1986)).

Defendants frequently do not perform the promised Phase 1 and Phase 2 services. Defendants do not take over communications and instead simply block the sextortionist. Defendants also fail to track the sextortionists' identities and location. Accordingly, Defendants do not prepare reports containing accurate information; Defendants place fabricated conversations and location coordinates in the promised reports, to conceal the fact they did not conduct the promised investigation.

Defendants commonly do not make any report to law enforcement regarding the sextortionist. Similarly, Defendants frequently do not perform any "monitoring" to detect renewed sextortion attacks. When Defendants' customers request a refund within the contractual time period, Defendants refuse to provide the promised refund amount or any refund at all.

Defendants represent that online reviews are truthful statements by Defendants' actual customers, when they are written entirely by Defendants. *See* Section II.H.

Thus, Defendants false representations violation Section 5 of the FTC Act as alleged in Counts I and II of the Complaint, Sections 310.3(a)(2)(iii) and 310.3(a)(4) of the TSR as alleged in Count III of the Complaint, and Section 521(a) of the GLB Act as alleged in Count IV of the Complaint.

b) Defendants Violate the Reviews & Testimonials Rule

The Reviews and Testimonials Rule prohibits a business from writing or creating a consumer review that materially misrepresents, expressly or by implication, that the reviewer exists. 16 C.F.R. § 465.2(a)(1). The Reviews and Testimonials Rule also prohibits a business from purchasing a consumer review about the business or one of the services it sells, which the business knew or should have known materially misrepresented, expressly or by implication, that

the reviewer exists, 16 C.F.R. § 465.2(b)(1), or that the reviewer used or had experience with the product, service, or business that is the subject of the review, 16 C.F.R. § 465.2(b)(2).

As discussed above at Section II.H, Defendants write, create, and purchase fake positive reviews that falsely represent that they are from Defendants' customers when they are not. Defendants wrote and created fake consumer reviews that were published online on ResellerRatings.com and a sextortion forum. Those reviews materially misrepresented that a genuine customer was posting a positive of Defendants' services when, in fact, Defendants wrote and created the reviews and no such customers actually exist. Furthermore, Defendants paid Uber drivers to assist with posting positive Google reviews regarding Defendants' services, while fully aware that the Uber drivers had no experience with Defendants' services.

Therefore, Defendants violate Sections 465.2(a)(1) and 465.2(b)(2) of the Reviews and Testimonials Rule, as alleged in Counts V and VI of the Complaint.

2. Corporate Defendants Act as a Common Enterprise and Are Jointly and Severally Liable for Each Other's Violations

Under the common enterprise theory, “[i]f the structure, organization, and pattern of a business venture reveal a ‘common enterprise’ or a ‘maze’ of integrated business entities, the FTC Act disregards corporateness.” *E.M.A. Nationwide*, 767 F.3d at 637 (quoting *FTC v. Wash. Data Res.*, 856 F.Supp.2d 1247, 1271 (M.D. Fla. 2012)). “Courts generally find that a common enterprise exists ‘if, for example, businesses (1) maintain officers and employees in common, (2) operate under common control, (3) share offices, (4) commingle funds, and (5) share advertising and marketing.’” *Id.* (quoting *Wash. Data Res.*, 856 F.Supp.2d at 1271). As set out in Section II.A, *supra*, the Corporate Defendants satisfy each of the common enterprise factors.

The same employees conduct business on behalf of multiple Corporate Defendants. The Chief Technology Officer for DFC incorporated several of the other Corporate Defendants. In addition to sharing numerous employees, the Corporate Defendants also share office space. Nearly all the Corporate Defendants list their primary business address as the main office building in Warrensville Heights, Ohio.

The Corporate Defendants jointly market the sextortion assistance services. The Corporate Defendants use dozens of websites that re-direct to each other. Often, customers will enter into a service agreement with one of the Corporate Defendants and receive receipts, correspondence, and other documentation from one or more additional Corporate Defendants. Belkin himself admits that consumers do not know who they are really doing business with, all they know is the name Digital Forensics.¹¹¹

The Corporate Defendants commingle funds. They frequently transfer and loan money back and forth among one another. Payments from consumers readily change hands to other Corporate Defendants.

Critically, all the Corporate Defendants operate under the common control of Belkin. He is either the registered agent, owner, or sole member of all Corporate Defendants except one. As to Cyber Digital, it is associated with a long-standing DFC employee, Viktor Sobiecki, and lists its business address as the same 4400 Renaissance address as the other Corporate Defendants, strongly implying that this entity is also under the control of Belkin.¹¹² Likewise, Belkin is the bank account signatory for all Corporate Defendants except Cyber Digital.

¹¹¹ Dilworth Decl. Ex. D at 33:12-22.

¹¹² In May and June 2026, Sobiecki received several large lump-sum payments. Smedley Decl. at ¶ 40.b. A former employee interviewed by the FTC stated that Belkin previously tried to make him incorporate new business entities and open bank accounts on Belkin's behalf. Smedley Decl. Ex. L at ¶ 15.

The evidence shows that there is no real distinction between the Corporate Defendants. *See FTC v. NHS Sys., Inc.*, 936 F. Supp. 2d 520, 533 (E.D. Pa. 2013). Accordingly, Corporate Defendants operated a common enterprise and are jointly and severally liable for harm caused by violations of the FTC Act.

3. Belkin Is Individually Liable for Injunctive and Monetary Relief

Defendant Belkin, the controlling force behind Defendants' scheme, is liable for the violations committed by Corporate Defendants. To obtain injunctive relief against an individual based on corporate violations of the FTC Act, the FTC must show that the "individual participated directly in the business entity's deceptive acts or practices, or had the authority to control them." *E.M.A. Nationwide*, 767 F.3d at 636 (quoting *FTC v. Freecom Commc'ns, Inc.*, 401 F.3d 1192, 1202 (10th Cir. 2005)). Authority to control the company 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 Serv.*, 875 F.2d 564, 573 (7th Cir. 1989), *overruled by FTC v. Credit Bureau Ctr., LLC*, 937 F.3d 764 (7th Cir. 2019). The FTC must also "show that the individual defendant knew or should have known of the alleged deceptive misrepresentation." *E.M.A. Nationwide*, 767 F.3d at 636 (quoting *Wash. Data Res.*, 856 F.Supp.2d at 1276). This knowledge element does not require subjective intent to defraud. *Int'l Computer Concepts*, 1995 WL 767810, at *5; *Amy Travel Serv.*, 875 F.2d at 574.

Additionally, to hold an individual liable for monetary redress, "the FTC must proffer evidence tending to show consumers actually relied on the entity's deceptive acts or practices to their detriment." *E.M.A. Nationwide*, 767 F.3d at 636. To raise a presumption of reliance, the FTC need only show the Corporate Defendants made material misrepresentations likely to

deceive consumers, which were widely disseminated, and consumers purchased Corporate Defendants' services. *See id.* at 631 n.12.

Belkin owns and controls the Corporate Defendants, which he uses to deceptively advertise and sell useless sextortion assistance services. He is the registered agent and bank account signatory for most of the Corporate Defendants. *See* Section II.A.

Belkin not only has the authority to control the Corporate Defendants, he participates directly in the Corporate Defendants' activities—Defendants' employees identify Belkin as the “mastermind” who drafted the deceptive telemarketing scripts and directed a scheme for posting fake reviews.¹¹³ *See* Section II.A. Corporate Defendants widely disseminated material misrepresentations to consumers through their websites and telemarketing calls. Thousands of consumers have purchased Corporate Defendants' services. Thus, there is a presumption consumers relied on the Corporate Defendants' misrepresentations. Accordingly, Belkin is liable for injunctive and monetary relief.

4. Irreparable Harm Exists

Where, as here, Defendants have allegedly violated multiple federal statutes, there is a “presumption of irreparable harm based on a statutory violation.” *City of New York v. Golden Feather Smoke Shop, Inc.*, 597 F.3d 115, 120 (2d Cir. 2010); *FTC v. World Wide Factors Ltd.*, 882 F.2d 344, 347 (9th Cir. 1987) (“irreparable injury must be presumed in a statutory enforcement action”). The passage of the FTC Act, GLB Act, and the Telemarketing Act are “in a sense, an implied finding that violations will harm the public and ought, if necessary, be restrained.” *United States v. Diapulse Corp of Am.*, 457 F.2d 25, 28 (2d Cir. 1972). Moreover,

¹¹³ Raffile Decl. ¶ 27; Dilworth Decl. ¶¶ 38-46; Smedley Decl. Ex. L at ¶¶ 12-13.

“concealment and dissipation of assets likely obtained through fraud constitutes irreparable harm[.]” *McGirr v. Rehme*, 891 F.3d 603, 613–14 (6th Cir. 2018). *See* Section II.C, *infra*.

5. The Balance of Equities Mandates Preliminary Injunctive Relief

In balancing the equities between the public and private interest, “the public interest should receive greater weight.” *Int’l Computer Concepts*, 1994 WL 730144 at *12 (citing 15 U.S.C. § 53(b)). Defendants are operating a fraudulent sextortion assistance scheme, *see* Section II, therefore their private interests have no weight. Defendants “can have no vested interest in [a] business activity found to be illegal.” *Diapulse Corp. of Am.*, 457 F.2d at 29 (internal quotations and citation omitted); *see also World Wide Factors*, 882 F.2d at 347.

Thus, the balance of the equities weighs in favor of granting the requested relief.

6. Injunctive Relief Will Serve the Public Interest

“The public interest in ensuring the enforcement of federal consumer protection laws is strong.” *FTC v. Mallett*, 818 F. Supp. 2d 142, 149 (D.D.C. 2011); *FTC v. Campbell Cap. LLC*, 2018 U.S. Dist. LEXIS 186728, at *7 (W.D.N.Y. Oct. 24, 2018) (finding “compelling public interest” in halting unlawful practices). Here, Defendants’ practices “demonstrate an ongoing pattern of law violations central to the success of defendants' business enterprise.” *Int’l Computer Concepts*, 1994 WL 730144, at *15.

Moreover, “the public interest in preserving the illicit proceeds . . . for restitution to the victims is great.” *FTC v. Affordable Media*, 179 F.3d 1228, 1236 (9th Cir. 1999); *see also Int’l Computer Concepts*, 1994 WL 730144, at *15 (finding public interest in injunctive relief where consumers suffered significant financial losses due to the defendants’ ongoing scheme). In this case, consumers have been conned out of thousands of dollars for Defendants’ useless services and Defendants will continue swindling more consumers in the absence of injunctive relief. A

temporary restraining order will serve the public interest by prohibiting Defendants from luring in new victims with false and deceptive statements, and preserve some possibility of redress for those consumers who have already been injured by Defendants' scheme.

Thus, all four factors weigh in favor of granting the requested relief.

C. An *Ex Parte* TRO with Additional Equitable Relief Is Necessary to Provide Final Effective Relief

The FTC requests an *ex parte* TRO that: (1) enjoins Defendants' unlawful conduct; (2) freezes assets; (3) appoints a temporary receiver; (4) grants immediate access to business premises and records; and (5) authorizes limited expedited discovery. As set out above, the evidence shows that the FTC is likely to succeed in proving that Defendants have been engaging in deceptive and unfair practices in violation of the FTC Act, the TSR, the GLB Act, and the Reviews and Testimonials Rule. Consumers will continue to suffer irreparable harm in the absence of injunctive relief. The balance of the equities and the public interest strongly support entry of preliminary injunctive relief. Thus, preliminary injunctive relief, including a temporary restraining order, is necessary and justified.

1. Conduct Relief Is Necessary to Stop Ongoing Consumer Harm

Conduct Relief is necessary to immediately stop ongoing consumer harm and falls squarely within this Court's injunctive authority under Section 13(b). The proposed TRO prohibits Defendants from making misrepresentations about their sextortion assistance services, from making false statements to obtain customer information of a financial institution, and from creating or paying for fake customer reviews. These measures simply require Defendants to comply with the law and are squarely within the Court's injunctive authority under Section 13(b) of the FTC Act.

2. An Asset Freeze Is Critical to Preserve the Possibility of Final Relief

Further, an asset freeze is necessary to preserve the possibility of restitution. “[T]o obtain an asset freeze, Plaintiff must show that ‘the asset freeze is reasonably necessary in order to preserve the possibility of complete and meaningful relief at the conclusion of litigation.’” *Foreclosure Sols.*, 2008 WL 11380125, at *6 (quoting *FTC v. Solar Michigan, Inc.*, 1988-2 Trade Case. (CCH) P68,339 (E.D. Mich. 1988)). The FTC brings this action under Section 19 in addition to Section 13(b).¹¹⁴ Section 19 authorizes the Court to grant such preliminary and final relief as the Court finds necessary to redress injury to consumers resulting from violations of FTC trade regulation rules. 15 U.S.C. § 57b. This relief may include the refund of money, among other things. *Id.*

To preserve the possibility of consumer redress at the conclusion of this case, it is necessary to impose an asset freeze to prevent Defendants from concealing or spending available funds. Financial records show Defendants dissipate assets, swiftly withdrawing or transferring most of the millions they swindle from consumers.¹¹⁵ The Corporate Defendants commingle the corporate assets. *See Foreclosure Sols., L.L.C.*, No. 1:08 CV 1075, 2008 WL 11380125, at *6 (N.D. Ohio Nov. 21, 2008) (granting preliminary injunction with an asset freeze based upon evidence suggesting the individual defendant was commingling the corporate defendant’s assets with the assets of individual defendant’s other businesses). Defendants regularly move the proceeds of their fraud overseas.¹¹⁶ Bank records also show that Defendants spend lavishly on luxury purchases and Belkin has spent more than \$38 million on personal credit card

¹¹⁴ *See FTC v. Elegant Sols., Inc.*, No. 20-55766, 2022 WL 2072735, at *2 (9th Cir. June 9, 2022).

¹¹⁵ Agarwal Decl. ¶ 21; Snell Rule 65(b)(1) Decl. ¶ 15.

¹¹⁶ Agarwal Decl. ¶ 18.

payments.¹¹⁷ Defendants will surely continue to dissipate assets in the absence of an asset freeze. “Without an immediate freeze of assets, it is unlikely that funds will be available to satisfy any final order granting restitution to defrauded consumers.” *Int'l Computer Concepts, Inc.*, 1994 WL 730144, at *16.

3. Appointment of a Temporary Receiver Is Appropriate

For the same reasons an asset freeze is necessary, the Court should appoint a temporary receiver to ensure preservation of assets and records. *Int'l Computer Concepts, Inc.*, 1994 WL 730144, at *17 (“Appointing a receiver is appropriate in a case such as this in which there is a risk that assets and records may be spirited away from the court's jurisdiction.”). Here, Defendants have a documented history of dissipating assets. Moreover, Defendants have substantial international ties, indicating a high likelihood that assets and records could be transferred outside the Court's jurisdiction. Belkin frequently travels internationally and the Corporate Defendants routinely transfer funds to international accounts. Courts in this district have previously appointed temporary receivers in cases where the FTC seeks a TRO and asset freeze.¹¹⁸

¹¹⁷ Agarwal Decl. ¶ 19; Smedley Decl. at ¶ 40.g-h (P&L statements for 1st All File Recovery USA, Inc. show boat and jetski).

¹¹⁸ See *FTC v. One or More Unknown Parties Deceiving Consumers*, No. 5:20-cv-2494 (N.D. Ohio Nov. 5, 2020), *FTC v. Repair All PC, LLC, et al.*, No. 1:17-cv-00869-DAP (N.D. Ohio Apr. 24, 2017); *FTC v. The Debt Advocacy Center, LLC, et al.*, No. 1:09 CV 2712 (N.D. Ohio Nov. 19, 2009); *FTC v. 6253547 Canada, Inc.*, No. 1:09 CV 1211 (N.D. Ohio June 2, 2009); *FTC v. 90I07-4021 Quebec, Inc.*, No. 1:08 CV 1051 (N.D. Ohio Apr. 25, 2008); *FTC v. Mazzoni & Son, Inc., d/b/a EDI Healthclaims Network, et al.*, No. 1:06 CV 2385 (N.D. Ohio Oct. 3, 2006); *FTC v. Hanson Pubs., Inc.*, No. 1:02 CV 2205 (N.D. Ohio Nov. 12, 2002); *FTC v. 1st Beneficial Credit Servs., LLC*, No. 1:02 CV 1591 (N.D. Ohio Aug. 14, 2002); *FTC v. Int'l Computer Concepts, Inc.*, No. 5:94-CV-1678 (N.D. Ohio Aug. 17, 1994).

4. It Is Necessary to Authorize Immediate Access to Defendants' Business Premises and Order Preservation and Production of Records

The FTC seeks preliminary relief designed to provide access to Defendants' records before they can be destroyed or concealed. As described herein, Defendants routinely fabricate evidence to conceal evidence of their wrongdoing. Defendants also take steps to conceal their identities, including when registering websites and when conducting business with consumers. *See* Sections II.A. The Proposed TRO allows for immediate access to Defendants' business premises to secure any assets and business records to ensure the Court's ability to review essential evidence and provide effective relief at the conclusion of this case. These procedures are appropriate and have been ordered *ex parte* relief in numerous FTC cases.¹¹⁹

5. Ex Parte Issuance Is Warranted

Federal Rule of Civil Procedure 65(b) permits *ex parte* orders upon a clear showing that "immediate and irreparable injury, loss, or damage will result" if the Court waits until defendants have notice. *Ex parte* orders are proper in cases "where notice to the defendant would render fruitless further prosecution of the action." *First Tech. Safety Sys., Inc. v. Depinet*, 11 F.3d 641, 650 (6th Cir. 1993). An *ex parte* order is justified where "the adverse party has a history of disposing of evidence or violating court orders or that persons similar to the adverse party have such a history." *Id.* at 650–51.

Defendants routinely destroy and falsify evidence to perpetuate their fraudulent schemes. Defendants defraud consumers using Phase 1 reports that contain fabricated evidence of an investigation Defendants did not actually conduct. *See* Section II.D. Defendants also falsified

¹¹⁹ *See, e.g., FTC v. Credit Glory LLC*, CV-26-05387-PHX-SPL, Dkt. 18 (D. Ariz. Aug. 4, 2026) (granting immediate access, receivership, and asset freeze); *FTC v. BlackRock Services, Inc.*, 8:25-cv-00363, Dkt. 2-1 (C.D. Cal. Feb. 27, 2025) (same).

documents provided in response to a law enforcement agency's subpoena and allegedly submitted false evidence in a lawsuit against a former employee.¹²⁰

The requested relief is appropriate and the Northern District of Ohio has previously granted the same relief under similar circumstances.¹²¹

IV. CONCLUSION

Defendants have repeatedly demonstrated they will not cease their unlawful activities despite many complaints and multiple inquiries from consumer protection agencies.

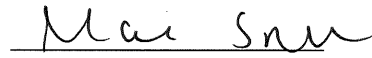
Accordingly—and because Plaintiff has demonstrated a likelihood of success and favorable equities—the Court should enter the proposed temporary restraining order to halt those activities and ensure injured consumers can receive effective final relief.

¹²⁰ See Section II.I; Snell Rule 65 Decl. ¶ 14 (discussing prior lawsuit against former employee).

¹²¹ See, e.g., *FTC v. Repair All PC, LLC*, No. 1:17-cv-00869-DAP (N.D. Ohio Apr. 24, 2017); *6253547 Canada, Inc.*, No. 1:09-CV-1211, 2009 WL 10714993, at *2–3 (N.D. Ohio June 2, 2009); *Int'l Computer Concepts*, No. 1:94CV1678, 1994 U.S. Dist. LEXIS 20965 (N.D. Ohio Oct. 24, 1994); *FTC v. 90I07-4021 Quebec, Inc.*, No. 1:08 CV 1051 (N.D. Ohio Apr. 25, 2008. see also *FTC v. E.M.A. Nationwide, Inc.*, 767 F.3d 611, 630 (6th Cir. 2014) (affirming *ex parte* temporary restraining order under the FTC Act).

Dated: October 5, 2026

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Maris Snell", written over a horizontal line.

Maris K.V. Snell
Federal Trade Commission
1350 Euclid Avenue, Suite 325
Cleveland, OH 44115
Phone: (202) 660-8544
E-mail: msnell@ftc.gov

Taylor H. Bates
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
Phone: (202) 326-2765
E-mail: tbates@ftc.gov

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION