

FILED

OCT 06 2026

CLERK U.S. DISTRICT COURT
NORTHERN DISTRICT OF OHIO CLEVELAND

**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. **1:26 CV 02615**

**COMPLAINT FOR PERMANENT
INJUNCTION, MONETARY
JUDGMENT, AND OTHER RELIEF**

JUDGE GAUGHAN

MAG JUDGE ARMSTRONG

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.

Plaintiff, the Federal Trade Commission (“FTC” or “Commission”), for its Complaint alleges:

1. The FTC brings this action for Defendants’ violations of 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, the FTC seeks relief, including a temporary, preliminary, and permanent injunction, monetary relief, and other relief, including an asset freeze, appointment of a receiver, and immediate access to Defendants’ business premises, pursuant to Sections 13(b) and 19 of the FTC Act, 15 U.S.C. §§ 53(b), 57b; Section 6(b) of the Telemarketing and Consumer Fraud and Abuse Prevention Act (“Telemarketing Act”), 15 U.S.C. § 6105(b); Section 522(a) of the GLB Act, 15 U.S.C. § 6822(a); and the Reviews and

Testimonials Rule.

SUMMARY OF THE CASE

2. Sextortion is a rapidly growing threat to Americans, routinely carried out by foreign scammers who target vulnerable individuals through digital channels.

3. In a financial sextortion attack, a cybercriminal threatens to publish a nude or sexual image (hereinafter, “explicit material”) of the victim unless the victim pays the criminal.

4. Sextortion victims experience extreme stress, fearing that release of the explicit material will devastate their personal lives, professional reputations, and relationships.

5. Federal law enforcement agencies, including the Federal Bureau of Investigation (“FBI”), warn that sextortion schemes increasingly target minors and young adults. To address the escalating harms from non-consensual intimate image (“NCII”) abuse, Congress enacted the Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (“TAKE IT DOWN Act”), which criminalizes the nonconsensual sharing of intimate images, including deepfakes, and requires covered platforms to remove NCII within 48 hours of a victim’s request. The FTC enforces platforms’ compliance with these provisions of the law.

6. Individuals experiencing sextortion attacks often turn to online search engines like Google for urgent help. Rather than finding law enforcement guidance and other free resources, victims frequently encounter Defendants’ advertisements and websites. Defendants capitalize on victims’ panic, employing fear-based sales scripts designed to escalate distress and compel immediate purchase of their services. For example, during sales calls, Defendants follow a script that plays on the victim’s individual “pain points”: if the victim is a military servicemember, Defendants warn that the sextortion attack can result in a dishonorable discharge; if the victim is

married, Defendants claim that the sextortionist will target the victim's spouse and in-laws; and if the victim is going through a divorce, Defendants explain that the sextortion attack can lead to loss of child custody or visitation rights.

7. Defendants falsely portray themselves as digital forensics experts, claiming they can track and identify sextortionists, prevent the spread of explicit material, and coordinate with law enforcement to bring criminals to justice. Defendants further mislead victims by asserting that law enforcement will not help stop the sextortion attack. Indeed, although the FBI has recommended for years that sextortion victims simply block and ignore sextortionists, Defendants tell victims that blocking the sextortionist is "the last thing you want to do."

8. Defendants induce victims to purchase expensive "Phase 1" sextortion assistance services costing between \$1,499 and \$20,000. Defendants represent that Phase 1 services include stopping the sextortion attack, taking over communications with the sextortionist, tracing the sextortionist's location through a "tracking campaign," producing a detailed investigative report, sending a cease-and-desist letter to the sextortionist, and reporting the sextortionist to law enforcement.

9. In fact, Defendants do not perform these services. Instead of communicating with the sextortionist through the victim's account, Defendants routinely change the victim's account settings simply to block the sextortionist's communications. Instead of obtaining investigative information, Defendants fabricate chat transcripts. Instead of tracing the sextortionist's location, Defendants reuse pre-saved geographic coordinates—often for Nigeria or the Philippines—and paste them into "Phase 1 Reports" and present these locations to victims as genuine results. Defendants also fail to contact law enforcement.

10. After victims pay for Phase 1, Defendants invariably pressure them to purchase an

additional “Phase 2” service that costs thousands of dollars more. Although Defendants claim Phase 2 is only needed in rare cases, in practice Defendants pressure every customer to pay for Phase 2. Defendants represent that, in the Phase 2 service, Defendants will monitor the victim’s accounts and the Internet to detect and defend against renewed attacks. Defendants also promise to report the sextortion attack to law enforcement. Defendants do not perform any of these services either.

11. Hundreds of consumers have complained about Defendants’ deceptive and abusive business practices. Many consumers complain directly to Defendants and request a refund, but Defendants often refuse to honor their contractual refund policy.

12. To conceal their failures and preserve the appearance of legitimacy, Defendants suppress negative reviews and generate positive fake reviews. Defendants direct dissatisfied customers to fake Better Business Bureau (“BBB”) websites operated by Defendants, ensuring negative reviews do not reach the real BBB. Defendants also coerce customers into removing negative reviews by conditioning partial refunds on signing non-disparagement agreements. Additionally, Defendants purchase fake positive reviews, including by paying Uber drivers to post fabricated testimonials using staged photos.

13. From February 2023 to July 2026, Defendants deceived consumers into paying at least \$60 million and, on information and belief, nearly all of Defendants’ income is from the sale of sextortion assistance services.

14. The FTC brings this action to stop Defendants’ unlawful conduct and seek relief for the consumers affected by Defendants’ unlawful business practices.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a),

and 1345.

16. Venue is proper in this District under 28 U.S.C. § 1391(b)(1), (b)(2), (c)(1), (c)(2), and (d), and 15 U.S.C. § 53(b).

PLAINTIFF

17. The FTC is an agency of the United States Government created by the FTC Act, which authorizes the FTC to commence this district court civil action by its own attorneys. 15 U.S.C. §§ 41–58. The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC also enforces the Telemarketing Act, 15 U.S.C. §§ 6101–6108, as amended. Pursuant to the Telemarketing Act, the FTC promulgated and enforces the TSR, 16 C.F.R. Part 310, as amended, which prohibits deceptive and abusive telemarketing acts or practices in or affecting commerce. The FTC also enforces Section 521(a) of the GLB Act, 15 U.S.C. § 6821(a)(2), which prohibits “making a false, fictitious, or fraudulent statement or representation” to obtain or attempt to obtain from a customer the “customer information of a financial institution.” The FTC also enforces the Reviews and Testimonials Rule, 16 C.F.R. Part 465, which prohibits businesses from creating or disseminating fake or false consumer reviews or testimonials.

DEFENDANTS

18. Defendant Digital Forensics Corporation, LLC (“DFC”) is an Ohio limited liability company with its principal place of business at 4400 Renaissance Parkway, Suite 1, Warrensville Heights, Ohio. DFC transacts or has transacted business in this District and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, DFC has advertised, marketed, distributed, or sold sextortion assistance services to consumers throughout the United States.

19. Defendant 1st All Data Recovery LLC (“1st All Data Recovery”), also doing business as Digital Forensics Corp, is a Florida limited liability company. 1st All Data Recovery is registered as a foreign for-profit company in the state of Ohio, with an office location at 3570 Warrensville Center Road, Suite 211, Shaker Heights, Ohio. 1st All Data Recovery transacts or has transacted business in this District and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, 1st All Data Recovery has advertised, marketed, distributed, or sold sextortion assistance services to consumers throughout the United States.

20. Defendant 1st All File Recovery USA, Inc. (“1st All File Recovery”), also doing business as Digital Investigation, File Recoup; Cyber Blackmail 911; and Digital Forensics; is an Ohio corporation with its principal place of business at 4400 Renaissance Parkway, Suite 1, Warrensville Heights, Ohio. 1st All File Recovery transacts or has transacted business in this District and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, 1st All File Recovery has advertised, marketed, distributed, or sold sextortion assistance services to consumers throughout the United States.

21. Defendant I & D Belkin LLC (“I & D Belkin”), also doing business as Data Recovery Services and Digital Forensics Corp, is an Ohio limited liability company with its principal place of business at 3570 Warrensville Center Road, Suite 211, Shaker Heights, Ohio. I & D Belkin transacts or has transacted business in this District and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, I & D Belkin has advertised, marketed, distributed, or sold sextortion assistance services to consumers throughout the United States.

22. Defendant Remote Backup Corp, LLC (“Remote Backup Corp”), also doing

business as Digital Cyber Forensics Investigation, is an Ohio limited liability company with its principal place of business at 4400 Renaissance Parkway, Suite 1, Warrensville Heights, Ohio. Remote Backup Corp transacts or has transacted business in this District and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Remote Backup Corp has advertised, marketed, distributed, or sold sextortion assistance services to consumers throughout the United States.

23. Defendant Digital Cyber Forensics Investigations LLC (“Cyber Investigation”), also doing business as Cyber Investigation, is an Ohio limited liability company with its principal place of business at 4400 Renaissance Parkway, Suite 1, Warrensville Heights, Ohio. Cyber Investigation transacts or has transacted business in this District and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Cyber Investigation has advertised, marketed, distributed, or sold sextortion assistance services to consumers throughout the United States.

24. Defendant Cyber Digital Forensics Response LLC (“Cyber Digital”) is an Ohio limited liability company with a registered address at 25101 Chagrin Boulevard, Suite 220, Cleveland, Ohio. Cyber Digital transacts or has transacted business in this District and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Cyber Digital has advertised, marketed, distributed, or sold sextortion assistance services to consumers throughout the United States.

25. Defendant 1st All Investments, LLC (“1st All Investments”) is an Ohio limited liability company with its principal place of business at 5755 Granger Road, Independence, Ohio. 1st All Investments transacts or has transacted business in this District and throughout the United States.

26. Defendant Salon Place LLC (“Salon Place”) is an Ohio limited liability company with its principal place of business at 4400 Renaissance Parkway, Suite 1, Warrensville Heights, Ohio. Salon Place transacts or has transacted business in this District and throughout the United States.

27. Defendant VPR Academy LLC (“VPR Academy”) is an Ohio limited liability company with its principal place of business at 4400 Renaissance Parkway, Suite 1, Warrensville Heights, Ohio. VPR Academy transacts or has transacted business in this District and throughout the United States.

28. Defendant 21111 Chagrin Investments LLC (“Chagrin Investments”) is an Ohio limited liability company with its principal place of business at 4400 Renaissance Parkway, Suite 1, Warrensville Heights, Ohio. Chagrin Investments transacts or has transacted business in this District and throughout the United States.

29. Defendant 4350 Renaissance LLC (“4350 Renaissance”) is an Ohio limited liability company with its principal place of business at 4400 Renaissance Parkway, Suite 1, Warrensville Heights, Ohio. 4350 Renaissance transacts or has transacted business in this District and throughout the United States.

30. Defendant Dmitry Belkin (“Belkin”) is the founder of DFC. Belkin is the registered agent of DFC, 1st All Data Recovery, Remote Backup Corp, 1st All Investments, VPR Academy, and Salon Place. Corporate filings list Belkin as a general partner of 1st All File Recovery and the sole member of 1st All Data Recovery, 1st All Investments, I & D Belkin, VPR Academy, and Chagrin Investments. In corporate filings and bank records, Belkin identifies himself as the owner of 1st All File Recovery, Remote Backup Corp, I & D Belkin, 1st All Investments, Cyber Investigation, Salon Place, VPR Academy, and 4350 Renaissance. Belkin is

the signatory on bank accounts in the names of 1st All Data Recovery, 1st All File Recovery, I & D Belkin, Remote Backup Corp, Cyber Investigation, 1st All Investments, VPR Academy, Salon Place, Chagrin Investments, and 4350 Renaissance.

31. At all times relevant to this Complaint, acting alone or in concert with others, Belkin has formulated, directed, controlled, had the authority to control, or participated in the acts and practices of DFC, 1st All Data Recovery, 1st All File Recovery, I & D Belkin, Remote Backup Corp, Cyber Investigation, Cyber Digital, 1st All Investments, Salon Place, VPR Academy, Chagrin Investments, and 4350 Renaissance, including the acts and practices described in this Complaint.

32. Belkin created and implements Defendants' business model, including, for example, what Defendants promise to consumers, how Defendants obtain consumers' payment information, and how to improve or manage Defendants' public corporate reputation. Belkin is solely responsible for drafting Corporate Defendants' telemarketing scripts, which contain the false and deceptive claims or representations Defendants make during sales calls with sextortion victims. Belkin devised and orchestrated Defendants' scheme of paying Uber drivers to create and post fake positive reviews for Defendants' services. Belkin has communicated directly with BBB representatives regarding concerns that Defendants were involved in submitting fake positive reviews for publication and that Defendants were taking improper actions to suppress customer complaints. Belkin resides in this District and, in connection with the matters alleged herein, transacts or has transacted business in this District and throughout the United States.

COMMON ENTERPRISE

33. Defendants DFC, 1st All Data Recovery, 1st All File Recovery, I & D Belkin, Remote Backup Corp, Cyber Investigation, Cyber Digital, 1st All Investments, Salon Place, VPR

Academy, Chagrin Investments, and 4350 Renaissance (collectively, “Corporate Defendants”) have operated as a common enterprise while engaging in the deceptive acts and practices and other violations of law alleged below. Corporate Defendants have conducted the business practices described below through an interrelated network of companies that have common ownership, officers, managers, business functions, employees, and office locations, that have commingled funds, and shared advertising and marketing. Because these Corporate Defendants have operated as a common enterprise, each of them is liable for the acts and practices alleged below.

34. Corporate Defendants disguise their true identities by operating under fictitious business names. Corporate Defendants often use or operate under the same or similar fictitious business names. For example, 1st All File Recovery, 1st All Data Recovery, and I & D Belkin all do business under the name “Digital Forensics” or a variation thereof, making much of their business activities indistinguishable from those of the actual DFC entity. Likewise, Remote Backup Corp does business under the name Digital Cyber Forensics Investigation, which is a name indistinguishable from that of Corporate Defendant Digital Cyber Forensics Investigations LLC.

35. Corporate Defendants also jointly advertise their sextortion assistance services under the name DFC. For example, corporate records reflect 1st All Data Recovery, 1st All File Recovery, and I & D Belkin collectively spending over \$17.5 million on advertising in 2024 and 2025, but online advertisements do not use the names of those three entities. On information and belief, these advertising expenses paid for advertisements of sextortion assistance services sold by “DFC.”

36. Corporate records for Corporate Defendants 1st All File Recovery, Remote

Backup Corp, Cyber Investigation, VPR Academy, and Chagrin Investments all list 4400 Renaissance Parkway, Suite 1, Warrensville Heights, Ohio 44128 as their registered office address. Bank records for Cyber Investigation, I & D Belkin, Remote Backup Corp, 1st All Investments, Salon Place, VPR Academy, Chagrin Investments, and 4350 Renaissance all list 4400 Renaissance Parkway, Suite 1, Warrensville Heights, Ohio 44128 as the office address. Corporate records for Corporate Defendants 1st All Data Recovery, 1st All File Recovery, I & D Belkin, and Salon Place have also listed the business's registered address as 3570 Warrensville Center Road, Suite 211, Shaker Heights, Ohio 44122.

37. In addition to Individual Defendant Belkin's authority over Corporate Defendants, the Corporate Defendants share officers and employees. Consumer complaints against Corporate Defendant Cyber Investigation reference multiple employees who are also employees of DFC. Incorporation documents for Corporate Defendant Cyber Digital list the contact information for DFC's long-standing Chief Technology Officer. DFC's General Counsel also serves as the registered agent for Chagrin Investments and submitted a fictitious name filing on behalf of Corporate Defendant Cyber Investigation.

38. Corporate Defendants commingle funds. For example, bank statements show multiple \$100,000 deposits from Cyber Digital to 1st All Data Recovery in February 2026. 1st All Data Recovery's September 2025 balance sheet shows a \$230,000 loan to Digital Cyber Forensics, presumably meaning Corporate Defendant Cyber Investigation. I & D Belkin's September 2025 balance sheet shows a \$400,000 loan from Remote Backup Corp. Cyber Investigation received a \$230,000 loan from I & D Belkin. Chagrin Investments' August 2025 balance sheet shows a \$654,564.59 loan to 1st All Data Recovery, a \$43,523.00 loan to 1st All File Recovery, and an \$11,085.20 loan to 1st All Investments. 4350 Renaissance's October 2025

balance sheet reflects loans to 1st All Investments, for \$185,000, and 1st All File Recovery, for \$389,339.43, and loans from 1st All Data Recovery, for \$20,000, and 1st All Investments, for \$4,188.45.

COMMERCE

39. At all times relevant to this Complaint, Defendants have maintained a substantial course of trade in or affecting commerce, as “commerce” is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

DEFENDANTS’ BUSINESS ACTIVITIES

40. Since at least 2020, Defendants have falsely and deceptively advertised and sold their sextortion assistance services to consumers throughout the United States.

Defendants’ Predatory Sextortion Assistance Services

41. Defendants operate multiple websites—including BlackmailHelpline.com, DigitalForensics.com, CyberBlackmail911.com, SecurityBreach911.com, and others—which target consumers searching for help during a sextortion crisis.

42. Defendants’ advertisements appear prominently on Google, YouTube, X, and other platforms when consumers search for help with an ongoing sextortion attack. Consumers frequently report that they found Defendants’ advertisements while still in a state of panic. As described by one consumer:

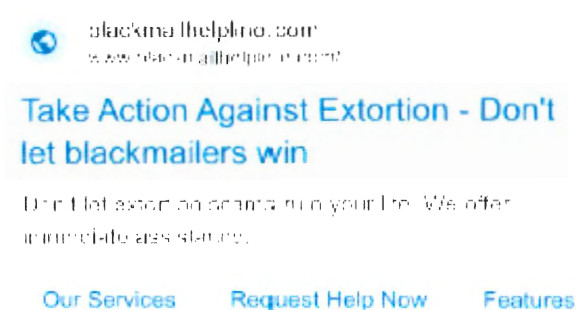
I was a victim of blackmail and sextortion. I was scared beyond belief and experiencing severe anxiety and panic attacks following the event. . . . I immediately searched for experts on the subject. Digital Forensics was the first result on the list. . . . During the initial call (about 12 hours after this happened to me) they scared me into thinking this was going to ruin my entire life. They made up a lot of things that I believed to be true. That they were 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. . . . I spent the next couple days trying to remain calm. Fighting off panic attacks and suicidal thoughts (partially induced by the companies

[sic] fear-mongering).

Defendants Falsely Advertise Their Sextortion Assistance Capabilities

43. Defendants' advertisements present Defendants as capable of offering immediate assistance to stop sextortion attacks. For example, Figure 1 below is a screenshot of a BlackmailHelpLine.com advertisement that appeared on Google, telling victims, "Don't let extortion scams ruin your life. We offer immediate assistance."

Figure 1: Example of Defendants' Google Ad



44. Defendants' ads further depict Defendants as experts in digital forensic services. Figure 2 below is a screenshot from one of Defendants' video advertisements posted on YouTube, titled "Sextortion and Black Mail," depicting Defendants' office as a sterile, laboratory-like environment.

Figure 2: Defendants' Video Advertisement "Sextortion and Black Mail"



45. Defendants make numerous representations about their experience and capability to help sextortion victims. Defendants advertise that they can “track down cyber criminals across the world through the use of our proprietary technology.” Defendants further promise, “Our proprietary IP to location ID process enables us to track down the IP addresses, service providers, and geographic location of these criminals. With that information we work with local authorities to bring criminals to justice and halt the harassment.”

46. Defendants’ advertisements, including the Sextortion and Black Mail video advertisement, advise sextortion victims not to pay the sextortionist. Instead, Defendants instruct victims to contact Defendants “right away” to let the experts “fight back.” Victims are directed to call Defendants’ phone numbers or visit one of Defendants’ websites.

47. For example, Figure 3 is a collection of excerpted screenshots from Defendants' website BlackmailHelpline.com, where Defendants tout their ability to "track down cyber criminals across the world [and] beat them," and to "identify [perpetrators] with a high degree of success [and] give law enforcement the evidence they need to make arrests."

Figure 3: Representations on Defendants' Website BlackmailHelpline.com

One of our specialties is investigating sextortion cases. We are able to track down cyber criminals across the world through the use of our proprietary technology. We know their tactics, and we know how to beat them. We have a success rate of more than 90 percent for keeping these criminals from ever sharing our clients' personal and private images and information.

How We Track Down Blackmailers?

Individuals, small businesses and large corporations are open to these online attacks. In such cases, the perpetrators hide their identities, attacking you from the internet shadows. We can expose them.

Our proprietary system lets us follow the digital footprints to track down IP addresses, cell phone numbers, email addresses, social media accounts and even specific devices used in these crimes. We can identify online harassers or extortionists with a high degree of success.

Identify Criminals

We can track down the IP addresses and geographic locations of the people harassing you.

Prevent Exposure

We give law enforcement the evidence they need to make arrests and keep explicit images offline.

48. As shown in Figure 3, Defendants also tout their ability to "prevent exposure" or the release of sextortion victims' explicit material, claiming that they can "keep[] these criminals from ever sharing our clients' personal and private images and information," and can "keep explicit images offline."

49. Figure 4 is a collection of excerpted screenshots from the same website, BlackmailHelpline.com, showing various scare tactics Defendants use to convince sextortion victims that they are facing dire consequences from the sextortion attack and need immediate assistance. As shown in the first screenshot, Defendants suggest that sextortionists will publish the victim's compromising material on the Internet and continue to demand money from the victim. Defendants warn that sextortionists' tactics "virtually guarantee[] people will see" the victims' explicit material. In the next screenshot, Defendants remind sextortion victims of the "horrific" repercussions if a sextortionist publicly releases the victim's explicit material, claiming that disclosure could result in "divorce or loss of parental rights." Defendants also caution that victims could "lose [their] job" and their "professional reputation could be destroyed."

Figure 4: Scare Tactics on Defendants' Website BlackmailHelpline.com

Sextortionists can be ruthless, and they are always changing how they operate. Some now create new websites, posting the victim's personal information — name, address, phone number and other details — along with the explicit video or images. The criminals use Search Engine Optimization techniques, and soon these sites begin to rank on major search engines such as Google, Bing and Yahoo. That means anyone searching the victim's name will run across that website with the explicit material on the very first page of search results, virtually guaranteeing people will see it.

The criminals then send a sextortion email or text, demanding payment to get the site taken down. If you pay them, though, they will simply put the page up again later and demand more money.

What can you do? Act swiftly, and call us.

WHY CHOOSE US

Don't Let Sextortionists Destroy Your Family Life and Reputation

What happens if someone shares your personal, explicit photos or video online? The risks are horrifying:

- ✓ **FAMILY**
Your family life could be in ruins, possibly even leading to divorce or loss of parental rights.
- ✓ **JOB**
Your professional reputation could be destroyed. You could even lose your job.
- ✓ **FRIENDS**
You could lose the trust of friends. They might never look you in the eye again.

CALL: 888.264.4131

50. Figure 5 is a screenshot showing representations made on Defendants' website DigitalForensics.com. As shown in Figure 5, Defendants suggest that only Defendants can help victims "recover" from the sextortion attack because paying the sextortionist and contacting law enforcement for help will not work: "The fee won't make them go away . . . [T]he legal system and police won't help either."

Figure 5: Representations on Defendants' Website DigitalForensics.com

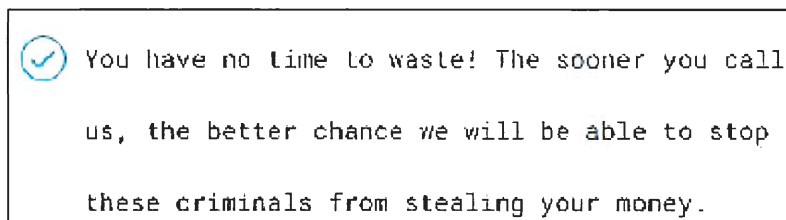
REPORT ONLINE SEXTORTION TO STOP THIS CRIME. LET US HELP YOU STAY SAFE.

We've helped many people recover from sextortionist online and protect both their family life and reputation.

The fee won't make them go away, so scammers will continue with their threats. Unfortunately, the legal system and police won't help either.

51. Figure 6 is a collection of screenshots from Defendants' website DigitalForensics.com, which instructs sextortion victims to contact Defendants. Defendants create a sense of urgency, advising sextortion victims to contact Defendants immediately, as shown in the first screenshot in Figure 6: "You have no time to waste!"

Figure 6: Instructions to Contact Defendants on Website DigitalForensics.com


A screenshot of a web form titled "Report Sextortion" in white text on a blue background. Below the title, it says "Response within 10 minutes" in smaller white text. The form contains several input fields: "First Name", "Last Name", "Phone", "Zip Code", and "Email". Below these is a larger text area with the placeholder text "Tell us how we can help in detail". At the bottom of the form is a prominent red button with the white text "REPORT SEXTORTION".

52. As shown in the second screenshot in Figure 6, the victim is prompted to fill out a "REPORT SEXTORTION" form with their name, contact information, and the details of their sextortion attack. Soon after the victim submits the form—often within 10 to 20 minutes—one of Defendants' sales representatives will call the victim.

Defendants Rely on Scare Tactics During Telemarketing Calls

53. When Defendants contact victims, they stick to a telemarketing script drafted by Defendant Belkin and designed to scare victims into purchasing Defendants' sextortion assistance services. The script requires DFC employees to use particular phrases, referred to as "pain points," that target the victim's fears and vulnerabilities.

54. For example, as shown in the first two excerpts in Figure 7, Defendants' script implies that if the victim's explicit material is released, the victim could face legal repercussions because the sextortionist will likely alter or photoshop the victim's private photos to make it look like the victim was involved in a sexual situation with a minor. At the end of each sales call, Defendants' employees must check the box shown in the third excerpt of Figure 7 to confirm that they used specific "keywords," including the word "pedophile," during every sales call with a sextortion victim.

Figure 7: Excerpts of Defendants' Telemarketing Script

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.

Say: In this situation we want to make sure we can protect all aspects of your life as quickly and discretely as possible. I've seen these situations ruin people's retirement all from the accusations of being a child predator. We need to make sure nothing gets posted.

Keywords (3+):
Embarrassment,
pedophile, you are a
paycheck to them, they
will not stop,
devastating
consequences, ruin your
life, no coming back
from this, life-altering

55. Consumers report that Defendants told them that the sextortionist will send the altered photos to the police, the victim's employer, or the victim's family and friends.

56. During a recorded undercover call with an FTC investigator posing as a sextortion victim, a DFC sales agent advised that blocking or ignoring the sextortionist could cause the sextortionist to fabricate damaging content and release it to family, friends, or employers. The DFC representative explained:

Another common tactic that these criminals use when you start blocking them and deleting them or even ignoring them is they'll start creating simple, free websites or even social media posts that will contain the victim's images, chats, and personal information. They even go as far as fabricating content to make it seem that their victims are trying to meet up with minors or doing unsavory acts with children where they will start posting this link to the webpage on social media [or send it] to family and friends or even sending them to your employer acting [as] a concerned parent who caught somebody sending photos to their underage son. Now, this is an extremely common tactic we've seen these criminals use in order to pressure the victims into paying. Now, we've even seen these pages start ranking on Google and Yahoo! so it becomes visible for online searches.

This threatening claim is consistent with Defendants' warning posted on BlackmailHelpline.com, as shown in the first screenshot in Figure 4, above.

57. Defendants' customers report how effective this tactic was during the initial sales call, as the following consumer complaint exemplifies:

Before going through the finances and plan details, the [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 [a] 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.

58. Defendants also leverage the sextortion victim's personal details to further increase the pressure. Defendants' sales scripts instruct employees to ask "probing questions" that are unrelated to the sextortion attack, such as whether the victim's marriage is "on the rocks, if infidelity has been an issue before, or if they have young kids that would mean a custody battle." Defendants then use the victim's answers during the sales pitch.

59. For example, if a victim mentions that they are married, Defendants will say something like, "We've seen these perpetrators [contact] spouses or partners, and they might even go after your in-laws because they know that that increases the damage tenfold[.]" Alternatively, if the victim mentions that they are going through a divorce and they have children, Defendants' employees are instructed to say the following:

I know you mentioned you were in the process of divorce and you had children together, this is the last thing you need the other party finding out about and trying to use against you. I have had clients in the past who have had this be the big factor in losing their divorce case and visitation rights. so our goal is to make sure we can start our investigation as soon as possible.

60. Defendants use information about the victim's career in the same way, claiming the victim will likely lose their job if the explicit material is released. Likewise, victims who are enlisted in the military are told that release of the explicit material will result in a dishonorable discharge, as the following telemarketing script excerpt shows:

Say: In this situation we want to make sure we can protect all aspects of your life as quickly and discretely as possible. If the extortionist were to send this out it can result in a dishonorable discharge, which will affect you even outside the military.

61. Defendants use details about the victim's sextortion attack in a similar manner. For example, during the FTC's undercover call, the FTC investigator shared that her sextortion attack began on Facebook. In response, the DFC sales agent told her, "Suspects from Facebook tend to be extremely aggressive with their efforts."

62. During sales calls, Defendants repeatedly emphasize that the victim cannot resolve the situation on their own, such as by blocking and ignoring communications from the sextortionist. As shown in the following excerpt from Defendants' sales script, Defendants expressly advise victims that ignoring the sextortionist "is not an option."

As I said prior, **ignoring them is not an option either**. This will piss them off and they will release the pictures/videos. Towards the end of this call we'll strategize **ways to hold off payment to the extortionist until we can take over**, we don't want these criminals getting a penny.

63. During the FTC's undercover call, DFC's representative warned that, due to the "severity" of the situation, blocking or ignoring the sextortionist is "the last thing that you want to do." The DFC representative reiterated: "Remember: they already have your phone number, and they already have your face These criminals have a lot of resources. . . . They'll come back with different accounts, different phone numbers, angry, and continue the extortion with more aggressiveness."

64. According to Defendants' former employees, at Belkin's instruction, Defendants monitor the sales calls closely to ensure employees do not deviate from these scripts. Employees that do not cover the "pain points" in every sales call face discipline, including having their compensation reduced.

65. After convincing victims that they cannot handle the situation on their own, Defendants detail their sextortion assistance services, which Defendants refer to as Phase 1 service and Phase 2 service.

Defendants' False Representations Regarding Phase 1 and Phase 2 Services

66. During the initial sales call, Defendants promise victims that Phase 1 is a comprehensive program designed to put an end to the sextortion attack. Indeed, the telemarketing scripts require the sales agent to tell potential customers that “the main goal of Phase 1 is simple: make these blackmailers stop[.]” During the FTC’s undercover call, DFC’s sales agent claimed that after Phase 1, “most of these criminals walk away.”

67. To further underscore the assurance that Defendants will stop the sextortion attack during Phase 1, Defendants claim during sales calls that their Phase 2 services are needed only in “rare” cases where the sextortionist is “more persistent.”

68. Based on Defendants’ telemarketing scripts, the FTC’s undercover call, and reports from consumers, Defendants promise to perform the following services in Phase 1:

- Log in to the victim’s social media, email, and other accounts to take over communication with the sextortionist;
- Conduct a “tracking campaign” to entice the sextortionist to click a link, which will reveal information about the sextortionist, potentially including the sextortionist’s name, identification, location, Internet Protocol (“IP”) address, Internet Service Provider (“ISP”), and other details;
- Compile all information gathered about the sextortionist into a “Phase 1 Report,” which will be provided to the victim;
- Send the sextortionist a cease and desist letter, which Defendants call a “gotcha letter,” to demonstrate to the sextortionist that Defendants are “in control of the situation since this letter includes all the information we’ve gathered on them, along with solid proof of their crimes being committed”; and

- Report the sextortionist's "illegal activities directly to authorities in their own countries," including the "local police department," which puts pressure on the sextortionist to end their attack.

69. Defendants Phase 1 service includes five service tiers ranging in price from \$1499 to \$20,000. For example, as shown in the chart below, the first tier costs \$1,499, and Defendants promise to begin work within six business days of payment, to be available to the victim during weekdays (from 9 a.m. to 9 p.m.), and to complete and provide the Phase 1 Report within 30 days of payment.

Cost	Start Work Within	Availability	Report Complete
\$1,499	6 business days	Mon – Fri, 9 a.m. – 9 p.m.	30 days
\$2,999	2 – 3 business days	Mon – Fri, 9 a.m. – 9 p.m.	15 days
\$4,999	24 – 48 hours	Mon – Sun, 9 a.m. – 12 a.m.	7 days
\$7,200	12 hours	Mon – Sun, 9 a.m. – 12 a.m.	3 days
\$20,000	Immediately	24/7	ASAP

70. Regardless of the victim's circumstances, Defendants' default recommendation is for the \$4,999 Phase 1 tier.

71. If a victim agrees to purchase the Phase 1 service, Defendants' employees are instructed to obtain payment information, including the customer's debit card or credit card numbers, and to process the consumer's payment before ending the phone call. Defendants typically charge customers an initial down payment, which is processed during the sales call, and then Defendants instruct customers to pay the remaining balance via wire transfer or certified check. Some consumers pay Defendants with personal checks containing the consumers' account numbers and routing numbers.

72. Defendants' practice is to send service contracts to customers for review and signature after receiving the customer's initial payment.

Defendants' Failure to Provide the Promised Sextortion Assistance Services

Defendants Often Do Not Perform the Phase 1 Services

73. After paying for Defendants' Phase 1 service, sextortion victims discover that the Phase 1 service is not what was promised.

74. In numerous instances, Defendants do not even attempt to complete the various services that were marketed and promised as part of Phase 1.

75. Defendants promise that they will log in to the victim's social media or other accounts used to communicate with the sextortionist and take over the communications. In fact, Defendants routinely log in to victims' accounts and simply block the sextortionist's communications, instead of communicating with the sextortionist as promised. Defendants block the sextortionists even though Defendants convince victims to pay thousands of dollars for Defendants to expertly handle communications with the sextortionist and expressly warn victims that blocking the sextortionist is "the last thing you want to do."

76. Defendants instruct clients not to log back into their own accounts during Defendants' "investigation," but several customers have reported that they ignored the instruction, logged into their accounts, and then were shocked to find that Defendants had simply blocked the sextortionist without ever communicating with the sextortionist.

77. In numerous instances, to convince customers that they communicated with the sextortionist, Defendants create fake or fictitious chat sessions that are intended to depict messages exchanged between Defendants and the sextortionist. In fact, the chat sessions are created by Defendants' employees. One of Defendants' former employees, who was a DFC sales

representative and manager, recalls observing other employees logging into communication platforms—like Facebook Messenger, WhatsApp, or Signal—and messaging each other back and forth to create a fabricated conversation between one of Defendants’ employees and another employee posing as the sextortionist. Defendants would then take a screenshot of the manufactured conversation and alter the image as necessary to make it look like a genuine conversation with the sextortionist had occurred.

78. Defendants then copy and paste the screenshots of the fake or doctored conversations into the Phase 1 Report, which purportedly summarizes all the findings of Defendants’ investigation and is provided to the customer.

79. Mark Tolok (“Tolok”), a former DFC “analyst” and “digital investigator,” corroborates that Defendants’ employees paste screenshots of fabricated or altered conversations into customers’ Phase 1 Reports, and notes that a manager reviews every report before it is provided to the customer. During his employment at DFC, Tolok observed Defendants’ employees altering or “photoshopping” the contents of messages exchanged with sextortionists and sharing those doctored conversations with customers. DFC’s employees are required to delete the entire chat log from the victim’s communication platform accounts, thereby preventing the victim from finding out the truth about Defendants’ communications, or lack thereof, with the sextortionist.

80. Defendants promise, as part of Phase 1, that they will send a “tracking link” to identify and locate the sextortionist and then send the sextortionist a cease and desist letter to intimidate the sextortionist into stopping their attack. In fact, in the numerous instances where Defendants block instead of communicate with the sextortionist, Defendants cannot and do not perform these services.

81. Sending the “tracking link” to obtain the sextortionist’s identity and location is a key aspect of Defendants’ marketing for the Phase 1 service. Defendants include the results of the “tracking campaign” in the Phase 1 Report, purporting to show the latitude and longitude coordinates of the sextortionist’s location. Figure 8 is a screenshot from one of Defendants’ Phase 1 Reports, supposedly identifying the sextortionist’s “Geographic Location Information” as Lagos, Nigeria.

Figure 8: Defendants’ Phase 1 Report Showing “Tracking Link Results”

TRACKING LINK RESULTS

IP address information is pivotal to the investigation because it provides a geolocation to the Suspect as well as their Internet Service Provider and device they are using.

No.	Time	Source	Destination
			102.89.23.91
			102.89.23.91
			102.89.23.91
			102.89.23.91

GEOGRAPHIC LOCATION INFORMATION

The Forensic Analyst notes that geolocation information obtained from an I.P. trace is not EXACT. This could be the closest cell tower, or network tower. These towers service areas anywhere from 500 feet to 5 miles in some locations.

 IP ADDRESS: 102.89.23.91

 COUNTRY: Nigeria

 REGION: Lagos

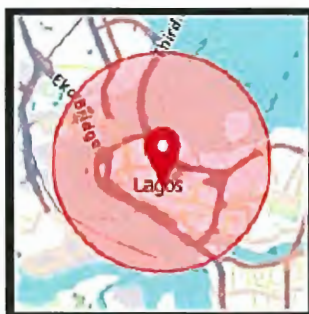
 CITY: Lagos

 ISP: MTN NIGERIA Communication limited

 ORGANIZATION:
MTNN-OJOTA-REGION-PREFIXES (mtn.com)

 LATITUDE: 6.4541

 LONGITUDE: 3.3947



82. In fact, former employees of Defendants estimate that half the “Tracking Link Results” shown in Phase 1 Reports are faked. For example, even when Defendants do send the sextortionist a tracking link, there are many instances when the sextortionist does not click on the link or the tracking link fails to obtain any useful information.

83. To conceal their failure to procure any legitimate tracking results, Defendants systematically include fabricated “evidence” in the Phase 1 Report provided to the customer. According to former employees, Defendants save the latitude and longitude coordinates for areas where sextortionists are known or believed to be commonly located, such as Nigeria and the Philippines, and Defendants simply reuse the same coordinates in the Phase 1 Reports.

84. Defendants also promise, as part of Phase 1, that they will report the sextortionist’s illegal activities directly to law enforcement authorities in the criminal’s home country, including the “local police department,” forcing the sextortionist to stop the attack. In fact, Defendants renege on this key promise; instead, they later insist that contacting law enforcement occurs only if the victim signs up for the Phase 2 service.

85. Defendants’ customers are dismayed when Defendants refuse to perform that critical aspect of the Phase 1 service. One consumer complainant reported as follows:

I was led to believe I was purchasing a complete investigative and legal solution, including both “discovery” and “action” phases. Only after payment did I learn that the “action” portion — the part involving actual legal takedown efforts — was not included and would cost thousands more.

86. Defendants rely upon this bait-and-switch tactic, along with renewed scare tactics, to coerce victims into paying even more for Phase 2 services.

Defendants Pressure Customers to Purchase Phase 2 Services

87. During the initial telemarketing calls, Defendants make false scripted representations to assure victims that Phase 1 services will almost certainly resolve the sextortion

attack and, therefore, the victims will not need to purchase additional Phase 2 services. For example, Defendants state during the initial sales calls that customers requiring Phase 2 services “doesn’t happen often” and that Defendants “rarely” recommend Phase 2 to customers.

88. In fact, Defendants subsequently pressure every customer to purchase Phase 2 services and a former employee estimates that Defendants’ pressure tactics succeed in convincing more than 50% of customers to sign up for Phase 2, which usually costs an additional \$2,000 to \$5,000 or more.

89. Numerous consumers have reported that Defendants called and harassed them into purchasing Phase 2 services. Defendants promise, as part of Phase 2, that they will (1) contact local law enforcement where the sextortionist lives to report the crimes and (2) monitor the victim’s accounts and the Internet in case the sextortionist renews the attack on the victim or releases the victim’s explicit material, and, in the event of a renewed attack, Defendants will address the situation.

90. The Phase 2 sales pitch is carefully crafted to convince clients that the sextortionist will likely return and resume the sextortion attack in the future, so ongoing protection from Defendants is needed.

91. For example, the following excerpt from a consumer complaint reflects an instance where Defendants pressured a consumer over the phone into purchasing Phase 2 services even though the sextortion attempts had ceased:

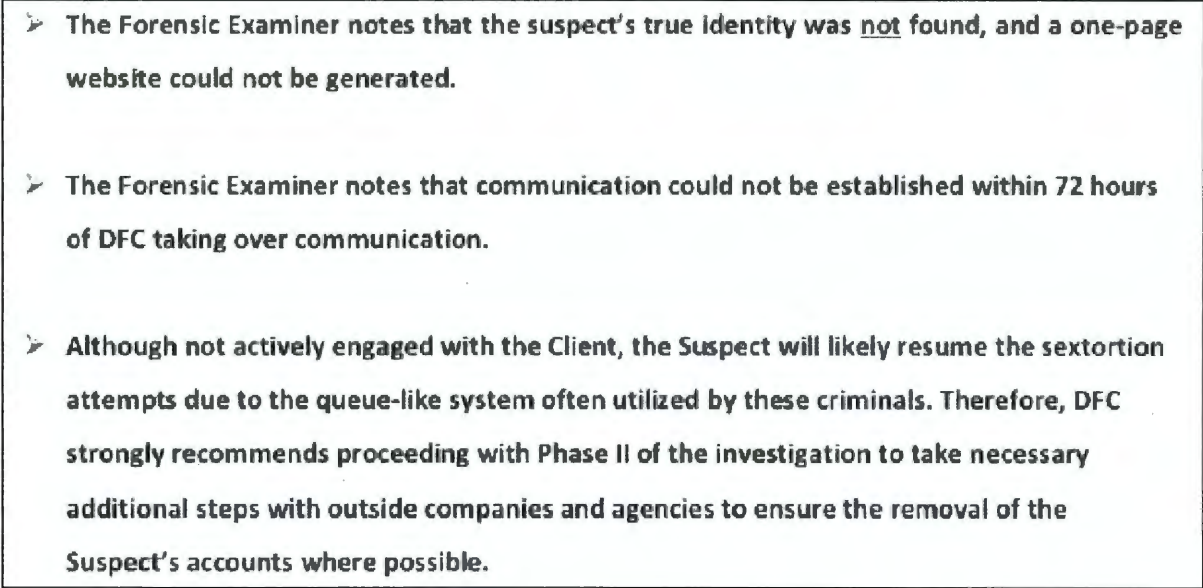
They told me if I wanted to continue after I need to pay for a PHASE 2. They have a certain way of trying to convince someone to pay for their service when they are reluctant. They try to fear monger the customer into believe [sic] insane scenarios that “may happen” The guy said things like the blackmailer could come back soon and send an AI picture of me with a minor . . . and, I will say, it scared the daylights out of me. Imagining my dignity and future life gone like that. It’s not who I am. So after being driven to fear by this person. I agreed to a 2 month plan which was supposed to be \$5k

92. Another consumer reported similar tactics, as follows:

I was sextorted [sic] and reached out to digital forensic corp and the[y] scared me in to signing up for phase 1 and . . . stated the[y] wo[u]ld be able to provide me with a name of the scammer and the location of said scammer witch [sic] they had told me was in Nigeria but couldn't get a name or photo after phase 1[.] they scarred [sic] me in to phase t[w]o by saying that the scammer can . . . make even police think that I was talking to a minor and that phase 2 would protect me from this information getting leaked but I started to fall behind they are threatening to sue me for the remaining balance of 12,486 dollars[.]

93. Defendants often recommend Phase 2 services based on the claim that the sextortionist "will likely resume the sextortion attempts," as shown in Figure 9 which is a screenshot from a Phase 1 Report.

Figure 9: Defendants' Phase 1 Report Recommendation

- 
- A screenshot of a Phase 1 Report Recommendation, enclosed in a black rectangular border. It contains three bullet points, each preceded by a right-pointing arrow. The text is in a bold, black, sans-serif font. The first bullet point states that the suspect's true identity was not found and a one-page website could not be generated. The second bullet point states that communication could not be established within 72 hours of DFC taking over communication. The third bullet point states that although not actively engaged with the client, the suspect will likely resume sextortion attempts due to the queue-like system often utilized by these criminals, and therefore, DFC strongly recommends proceeding with Phase II of the investigation to take necessary additional steps with outside companies and agencies to ensure the removal of the suspect's accounts where possible.
- **The Forensic Examiner notes that the suspect's true identity was not found, and a one-page website could not be generated.**
 - **The Forensic Examiner notes that communication could not be established within 72 hours of DFC taking over communication.**
 - **Although not actively engaged with the Client, the Suspect will likely resume the sextortion attempts due to the queue-like system often utilized by these criminals. Therefore, DFC strongly recommends proceeding with Phase II of the investigation to take necessary additional steps with outside companies and agencies to ensure the removal of the Suspect's accounts where possible.**

94. In numerous other instances, Defendants claim they discovered information about the sextortionist that necessitates Phase 2 services, as reflected in the following consumer complaint excerpts:

- "When they found out information on the criminal, they claimed he was a very vicious and aggressive type and I needed to move to phase two of the process which costed [sic]

another 3,000 dollars.”

- “I was informed that there is a 60% likelihood of me being contacted and possibly threatened some more. I was offered what they called a ‘Phase Two’ investigation package of 6 months for a total of about \$3,000[.]”
- “Digital Forensics Corp wants me to sign up for another plan that would cost as much to keep their efforts on going. I have run out of money. Digital Forensics Corp told me and shared a report with their findings. The sextortionist is out of Cote D’Ivoire. . . . [T]hey predict there is a 93% chance the sextortionist will reemerge again, demanding more money. I have nothing left.”

Defendants Do Not Actually Provide the Promised Phase 2 Services

95. After scaring customers and inducing them to pay thousands of dollars for Phase 2 services, in numerous instances, Defendants do not provide the promised services.

96. Indeed, former employees of Defendants attest that Defendants rarely contact local law enforcement to report sextortionists. Defendants tell consumers that Defendants have close relationships with law enforcement in foreign countries, but according to a former employee, Defendants simply use Google to search for publicly available contact information for law enforcement agencies.

97. Former employee Tolok states that even when Defendants send an email to a law enforcement agency, Defendants frequently receive a bounce-back message and take no further steps to contact the agency. Notably, even when letters or emails to law enforcement are delivered, there is no response and no law enforcement action is taken against the sextortionists. On information and belief, Defendants have never worked with law enforcement to secure an arrest of a sextortionist.

98. Former employees of Defendants also confirm that Defendants do not “monitor” customer accounts or the Internet, despite claiming to provide this service as a core component of Phase 2. Tolok refers to Defendants’ Phase 2 as a “scam” because “everyone internally knew nothing was really being done.”

Defendants’ Sextortion Assistance Services Are Ineffective

99. In numerous instances, Defendants fail to obtain any information that can be used to identify or locate sextortionists. Unsurprisingly, many consumers have reported that Defendants were not successful in stopping their sextortion attacks.

100. Consumers frequently report that, after they paid for Defendants’ sextortion assistance services, their sextortionist continued contacting them through new communication platforms or different phone numbers. Multiple customers have also reported that Defendants failed to prevent the sextortionist from publicly releasing their explicit material.

101. Defendants’ former employees admit that sextortionists would “very often” continue reaching out to the victims, and they recall multiple cases where the sextortionist exposed the victim’s explicit material even after the victim retained Defendants’ services.

102. Tolok also attests that Defendants’ claimed “90% success rate,” which Defendants reference on their websites and during telemarketing calls, is a “made up number.” Tolok clarifies that it was “really a matter of luck” whether the sextortion attack would stop after sextortion victims retained Defendants.

Defendants Often Refuse to Honor Their Refund Policy

103. Defendants’ sextortion assistance contracts generally provide as follows:

[A]ny refunds or cancellation requests will be handled in the following fashion:

Up [] to 75% refund: cancellation request made within 1 day after contract signed

Up [] to 50% refund: cancellation request made within 2 days after contract signed

Up [] to 25% refund: cancellation request made within 3 days after contract signed

104. Many customers have reported that Defendants fail to provide updates on the status of their case or respond to their questions. If customers request a refund, Defendants often cease communicating with them entirely. Despite including a refund policy in the sales contract, in numerous instances, Defendants have refused to honor their refund policy, even when customers requested a refund within the three-day refund period.

105. In some instances, customers have reported that Defendants took actions seemingly designed to prevent the customers from qualifying for a refund. For example, customers allege that Defendants instructed them not to contact Defendants for 72 hours after purchasing Defendants' services purportedly to allow Defendants to "investigate" their cases without interruption, but Defendants later denied these customers refunds since they were not requested within the three-day refund period. Many customers report that Defendants delayed responding to their refund requests until after the three-day refund eligibility period had expired. Customers also report that after they instructed Defendants to cancel their contract and stop working, Defendants continued working anyway and then used the excuse that work had been completed as the basis for denying the customers' refund requests.

106. In the uncommon instances where Defendants agree to provide a refund—which is almost always a small percentage of the total amount the sextortion victim paid—Defendants condition the refund on the customer signing Defendants' Release and Settlement Agreement containing a "non-disparagement" clause. The clause requires the customer to remove any negative reviews they previously posted online before they receive their refund. The Release and Settlement Agreement also contains a non-disclosure provision, a \$500-per-day liquidated

damages provision, and a clause requiring customers to pay Defendants' attorneys' fees.

Defendants Unlawfully Suppress Negative Reviews and Disseminate Fake Positive Reviews

107. In hundreds of instances, Defendants' customers have complained, including through the BBB, the FTC, and other law enforcement agencies, that Defendants fail to provide the sextortion assistance services they advertise and that Defendants do not successfully end sextortion attacks as promised.

108. Many consumers have described feeling re-victimized by Defendants' deceit. One consumer explained, "I was pressured by Digital Forensics to purchase their services. They essentially used the same tactics as the original extortion playing on my fears whenever I seemed hesitant to purchase their services." Another consumer stated that Defendants are "worse than the actual criminals."

109. Indeed, due to the large number of complaints against DFC, the BBB has posted multiple alerts on DFC's BBB business profile. Throughout the years, DFC and Belkin have asked the BBB to remove the alerts, but each time the BBB determined that the pattern of complaints had not declined and therefore denied DFC's requests.

110. In April 2021, the BBB added an additional alert noting that complaints filed against DFC "continue to show concerns with Phase 1 to Phase 2 misrepresentations, slow response to phone calls and emails, and delays in providing promised information by Digital Forensics." In December 2024, the BBB again alerted the public that many "complaints received still allege concerns with Phase 1 and Phase 2 promises."

Defendants Suppress Customers' Negative Reviews

111. To rehabilitate their public reputation, Defendants take actions to suppress negative reviews about their business practices.

112. According to a former employee, to prevent negative reviews, when Defendants perceive that a customer is “unhappy” or dissatisfied, they send the customer a link to a fake version of the BBB website, which Defendants operate and control. If the customer clicks on the link, they can submit a negative review on what appears to be the BBB website. However, the negative review will not be submitted to the BBB and instead will be redirected to Defendants, who do not publicize or otherwise act on the negative review. As the same former employee explains, Defendants are careful to email a genuine link to the BBB website only to customers they believe are “happy” with Defendants’ services.

113. Defendants also typically refuse to provide customers with a refund unless they sign a Release and Settlement Agreement and remove any negative review they posted previously regarding Defendants.

114. In June 2024, the BBB became aware of Defendants’ requirement that customers remove negative reviews to receive a refund. The BBB sent a letter to Belkin to advise him that the practice could violate the Consumer Review Fairness Act or, at minimum, reduce DFC’s BBB rating. Subsequently, the BBB added an alert to DFC’s BBB profile, noting that DFC’s practice raises “questions [] regarding the authenticity of reviews.”

Defendants Generate and Disseminate Fake Positive Reviews

115. According to Defendants’ former employee, Belkin devised and implemented a scheme to generate and disseminate fake positive reviews to improve Defendants’ public reputation. Belkin requires Defendants’ employees to assist with posting fake positive reviews on Google, using a process designed to circumvent Google’s mechanisms for detecting fake reviews.

116. Belkin instructed employees to mail packets of paper to randomly selected cities

throughout the United States, with the top page reading “Digital Forensics Corporation” in large letters. On information and belief, the packet is intended to appear like paperwork received from Defendants, such as a Phase 1 Report. Next, Belkin instructed employees to hire and pay an Uber driver in the city where the paperwork had been mailed. The Uber driver was instructed to pick up the paperwork, drive to an unoccupied office building nearby, and take a photo holding up the paperwork, showing “Digital Forensics Corporation” on the top page, with the office building in the background. Finally, the Uber driver was required to post a fake positive Google review about Defendants’ services and include the photo, which is intended to create the false impression that the Uber driver is a satisfied DFC customer leaving a meeting at one of Defendants’ locations.

117. According to Belkin, if the geolocation data for the photo corresponds with the location where the review was posted, Google will automatically authenticate and publicize the fake review. In multiple instances, Defendants followed this process and fake positive reviews regarding Defendants’ services were created and successfully posted on Google.

118. Defendants paid Uber drivers to post positive reviews regarding Defendants’ services when Defendants knew that the Uber drivers did not actually have any experience with Defendants’ services.

119. On information and belief, Defendants also wrote, created, or disseminated on the BBB website fake positive reviews regarding Defendants’ services. Beginning in early 2024, the BBB recognized an unusual pattern where multiple positive reviews for Defendants were submitted to the BBB shortly after a BBB complaint was filed against Defendants.

120. The BBB used multiple techniques to attempt to verify the positive reviews, but in almost every instance, the BBB was unable to confirm that a real person submitted the review.

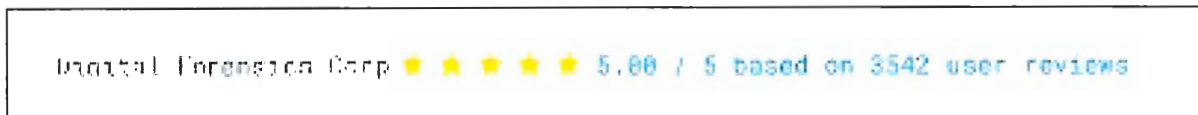
Due to the high rate of unverifiable positive reviews, the BBB took several precautions, including: (1) removing from the BBB's website all positive reviews that could not be authenticated and (2) refraining from posting new positive reviews to the BBB's website until the review was authenticated.

121. On June 3, 2024, the BBB sent a letter to Belkin describing the BBB's concerns with the "irregularities" in reviews submitted for DFC, explaining the BBB's decision to place an alert on DFC's BBB business profile due to the BBB's inability to "confirm the authenticity of numerous reviews submitted for [DFC]," and stating the BBB's decision to remove positive reviews that may have been affected by the lack of verifiable authenticity.

122. BBB personnel spoke with Belkin and DFC's General Counsel to discuss the pattern of unverifiable reviews. Defendants repeatedly attempted to persuade the BBB to post the unverifiable reviews.

123. As shown in Figure 10, on their website DigitalForensics.com, Defendants emphasize their trustworthiness by citing a supposed perfect 5 out of 5 stars rating based on 3,542 customer reviews.

Figure 10: Defendants' 5-Star Rating on DigitalForensics.com



124. However, a former DFC employee disclosed that DFC employees based in India write and post fake positive reviews to the website ResellerRatings.com. The positive reviews posted to this website serve as the basis for the "5 out of 5 stars based on 3542 user reviews" rating shown on DFC's website. Defendants know that the employees posting the positive reviews are not actual customers who have had a positive experience with Defendants' services.

125. Consumers have also reported that, after they paid for Defendants' sextortion assistance service, Defendants refused to provide the promised assistance until the consumer provided a screenshot proving that the consumer had submitted a positive BBB review regarding Defendants' services. Defendants knew that the consumers did not yet have experience with Defendants' services, but required the consumers to post false reviews claiming to have had a positive experience.

126. Based on the facts and violations of law alleged in this Complaint, the FTC has reason to believe that Defendants are violating or are about to violate laws enforced by the Commission.

VIOLATIONS OF THE FTC ACT

127. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

128. Misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices prohibited by Section 5(a) of the FTC Act.

129. As set forth below, Defendants have engaged and continue to engage in violations of Section 5(a) of the FTC Act in connection with the advertising, marketing, and sale of their sextortion assistance services.

COUNT I

Misrepresentations Regarding Defendants' Sextortion Assistance Services

130. In numerous instances in connection with the advertising, marketing, promotion, offering for sale, or sale of sextortion assistance services, Defendants represent, directly or indirectly, expressly or by implication, that:

- a. Defendants will stop the sextortion attack;

- b. Defendants will communicate with sextortionists on behalf of the customer;
- c. Defendants will conduct a “tracking campaign” that will obtain accurate details on the sextortionist, including the sextortionist’s identity and location;
- d. Defendants will provide the customer with a report containing truthful information collected about the sextortionist;
- e. Defendants will report the sextortionist’s illegal activities to law enforcement;
- f. Defendants will “monitor” the customer’s accounts and the Internet to detect and intervene in any renewed sextortion attack; and/or
- g. Defendants will provide the customer with a refund if it is requested within the time period set out in Defendants’ contracts.

131. In fact, in numerous instances in which Defendants have made the representations described in Paragraph 130:

- a. Defendants do not stop the sextortion attack;
- b. Defendants have blocked the sextortionist without ever communicating on behalf of the customer;
- c. Defendants do not communicate with the sextortionist, therefore Defendants could not have enticed the sextortionist to click a link and provide tracking information or, if Defendants did send a tracking link, it failed to provide any accurate tracking information;
- d. Defendants provide customers with reports containing inaccurate and/or fabricated information about the sextortionists;
- e. Defendants do not report sextortionists’ illegal activities to law enforcement;
- f. Defendants do not “monitor” customers’ accounts or the Internet to detect or

intervene in any renewed sextortion attack; and/or

- g. Defendants refuse to provide refunds even when a customer requests a refund within the time period set out in Defendants' contract.

132. Therefore, Defendants' representations as described in Paragraph 130 are false or misleading and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT II

Deceptive Consumer Reviews

133. Through the means described in Paragraphs 115–125, Defendants have represented, directly or indirectly, expressly or by implication, that positive reviews of Defendants' services posted to online platforms, including Google, the BBB's website, and ResellerRatings.com, are truthful reviews by actual customers of Defendants.

134. In fact, in numerous instances in which Defendants have made the representations described in Paragraph 133, the positive reviews of Defendants' services were not truthful reviews by actual customers, but instead were either: a) fabricated by individuals paid or otherwise induced by Defendants to provide positive reviews, b) provided by Defendants or Defendants' agents, or c) provided by customers coerced by Defendants into writing a positive review that did not reflect the customers' experiences, views, or opinions.

135. Therefore, Defendants' representations as described in Paragraph 133 are false or misleading and constitute a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

VIOLATIONS OF THE TELEMARKETING SALES RULE

136. In 1994, Congress directed the FTC to prescribe rules prohibiting abusive and

deceptive telemarketing acts or practices pursuant to the Telemarketing Act, 15 U.S.C. §§ 6101–6108. The FTC adopted the original TSR in 1995, extensively amended it in 2003, and amended certain sections thereafter. See 16 C.F.R. Part 310.

137. Defendants are “sellers” or “telemarketers” engaging in “telemarketing” as defined by the TSR, 16 C.F.R. § 310.2(ee), (hh), and (ii). A “seller” means “any person who, in connection with a telemarketing transaction, provides, offers to provide, or arranges for others to provide goods or services to the customer in exchange for consideration.” 16 C.F.R. § 310.2(ee). A “telemarketer” means “any person who, in connection with telemarketing, initiates or receives telephone calls to or from a customer or donor.” 16 C.F.R. § 310.2(hh). “Telemarketing” means a “plan, program, or campaign which is conducted to induce the purchase of goods or services or a charitable contribution, by use of one or more telephones and which involves more than one interstate telephone call.” 16 C.F.R. § 310.2(ii).

138. The TSR prohibits sellers and telemarketers from “[m]isrepresenting, directly or by implication, in the sale of goods or services” any material aspect of the goods or services that are the subject of a sales offer. 16 C.F.R. § 310.3(a)(2). Specifically, the TSR prohibits sellers and telemarketers from misrepresenting “[a]ny 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). Likewise, the TSR 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).

139. Pursuant to Section 3(c) of the Telemarketing Act, 15 U.S.C. § 6102(c), and Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the TSR constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of Section 5(a) of the

FTC Act, 15 U.S.C. § 45(a). Section 19(a)(1) of the FTC Act, 15 U.S.C. § 57b(a)(1), provides that the FTC may commence a civil action against “any person, partnership, or corporation” who “violates any rule . . . respecting unfair or deceptive acts or practices.” Section 19(b) of the FTC Act, 15 U.S.C. § 57b(b), provides that in any action commenced under Section 19(a)(1), the court “shall have jurisdiction to grant such relief as the court finds necessary to redress injury to consumers, including but not limited to rescission or reformation of contracts, the refund of money or return of property.”

COUNT III

Deceptive Telemarketing Calls in Violation of the TSR

140. In numerous instances, in connection with the advertising, marketing, promotion, offering for sale, or sale of sextortion assistance services, Defendants misrepresent, directly or indirectly, expressly or by implication, that:

- a. Defendants will stop the sextortion attack;
- b. Defendants will communicate with sextortionists on behalf of the customer;
- c. Defendants will conduct a “tracking campaign” that will obtain accurate details on the sextortionist, including the sextortionist’s identity and location;
- d. Defendants will provide the customer with a report containing truthful information collected about the sextortionist;
- e. Defendants will report the sextortionist’s illegal activities to law enforcement;
- f. Defendants will “monitor” the customer’s accounts and the Internet to detect and intervene in any renewed sextortion attack; and/or
- g. Defendants will provide the customer with a refund if it is requested within the time period set out in Defendants’ contracts.

141. Therefore, Defendants' acts or practices as described in Paragraph 140 are deceptive telemarketing acts or practices in violation of the TSR, 16 C.F.R. §§ 310.3(a)(2)(iii) and (a)(4).

VIOLATIONS OF THE GRAMM-LEACH-BLILEY ACT

142. Section 521 of the GLB Act, 15 U.S.C. § 6821, became effective on November 12, 1999, and remains in full force and effect. Section 521(a)(2) of the GLB Act, 15 U.S.C. § 6821(a), prohibits any person from “obtain[ing] or attempt[ing] to obtain, or caus[ing] to be disclosed or attempt[ing] to cause to be disclosed to any person, 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.”

143. The GLB Act defines “customer” to mean, “with respect to a financial institution, any person (or authorized representative of a person) to whom the financial institution provides a product or service, including that of acting as a fiduciary.” 15 U.S.C. § 6827(1). The GLB Act defines “customer information of a financial institution” as “any information maintained by or for a financial institution which is derived from the relationship between the financial institution and a customer of a financial institution and is identified with the customer.” 15 U.S.C. § 6827(2). The GLB Act defines a “financial institution” as “any institution engaged in the business of providing financial services to customers who maintain a credit, deposit, trust, or other financial account or relationship with the institution.” 15 U.S.C. § 6827(4)(A).

144. Section 522(a) of the GLB Act, 15 U.S.C. § 6822(a), empowers the FTC to enforce Section 521 of the GLB Act “in the same manner and with the same power and authority as the [FTC] has under the Fair Debt Collection Practices Act [FDCPA] . . . to enforce compliance with such Act.” Pursuant to Section 814(a) of the FDCPA, 15 U.S.C. § 1692l(a), a

violation of the FDCPA is deemed an unfair or deceptive act or practice in violation of the FTC Act. Section 814(a) of the FDCPA further provides that all of the functions and powers of the FTC under the FTC Act are available to the FTC to enforce compliance by any person with the FDCPA, including the power to enforce provisions of the FDCPA in the same manner as if the violation had been a violation of an FTC trade regulation rule. Thus, pursuant to Section 522(a) of the GLB Act, the FTC may enforce Section 521 of the GLB Act in the same manner as if a violation of the GLB Act were a violation of an FTC trade regulation rule.

145. Section 19 of the FTC Act, 15 U.S.C. § 57b, authorizes this Court to grant such relief as the Court finds necessary to redress injury to consumers resulting from Defendant's violations of the GLB Act, including, but not limited to, the rescission or reformation of contracts, and the refund of money or return of property.

COUNT IV

Use of False, Fictitious, or Fraudulent Statements to Obtain or Attempt to Obtain, or Cause to Be Disclosed or Attempt to Cause to Be Disclosed, Customer Information of a Financial Institution

146. In numerous instances in connection with the advertising, marketing, promotion, offering for sale, or sale of their sextortion assistance services, Defendants make and have made false, fictitious, or fraudulent statements or representations to customers of financial institutions to obtain or attempt to obtain, or to cause to be disclosed or attempt to cause to be disclosed, customer information of a financial institution, such as bank account numbers, credit card numbers, and debit card numbers, including by misrepresenting, directly or indirectly, expressly or by implication, that:

- a. Defendants will stop the sextortion attack;
- b. Defendants will communicate with sextortionists on behalf of the customer;
- c. Defendants will conduct a "tracking campaign" that will obtain accurate

details on the sextortionist, including the sextortionist's identity and location;

- d. Defendants will provide the customer with a report containing truthful information collected about the sextortionist;
- e. Defendants will report the sextortionist's illegal activities to law enforcement; and/or
- f. Defendants will "monitor" the customer's accounts and the Internet to detect and intervene in any renewed sextortion attack.

147. Therefore, Defendants' acts or practices as described in Paragraph 146 violate Section 521 of the GLB Act, 15 U.S.C. § 6821.

VIOLATIONS OF THE REVIEWS AND TESTIMONIALS RULE

148. The Reviews and Testimonials Rule took effect on October 21, 2024, and has since that date remained in full force and effect.

149. Defendants are individuals and corporations that sell products or services, therefore Defendants are a "business" as defined by the Reviews and Testimonials Rule, 16 C.F.R. § 465.1(a).

150. "Consumer review" means "a consumer's evaluation, or a purported consumer's evaluation, of a product, service, or business that is submitted by the consumer or purported consumer and that is published to a website or platform dedicated in whole or in part to receiving and displaying such evaluations." 16 C.F.R. § 465.1(d).

151. "Purchase a consumer review" means "to provide something of value, such as money, gift certificates, products, services, discounts, coupons, contest entries, or another review, in exchange for a consumer review." 16 C.F.R. § 465.1(m).

152. "Reviewer" means "the author or purported author of a consumer review."

16 C.F.R. § 465.1(n).

153. The Reviews and Testimonials Rule prohibits a business from writing or creating a consumer review or consumer testimonial that materially misrepresents, expressly or by implication, that the reviewer or testimonialist exists. 16 C.F.R. § 465.2(a)(1).

154. The Reviews and Testimonials Rule also prohibits a business from purchasing a consumer review about the business or one of the products or 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 otherwise had experience with the product, service, or business that is the subject of the review or testimonial, 16 C.F.R. § 465.2(b)(2).

155. Pursuant to Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the Reviews and Testimonials Rule constitutes an unfair or deceptive act or practice in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT V

Writing or Creating Fake or False Consumer Reviews and Testimonials

156. In numerous instances, through the means described in Paragraphs 115–124, Defendants have written or created a consumer review that materially misrepresents, expressly or by implication, that the reviewer exists.

157. Therefore, Defendants' acts or practices, as described in Paragraph 156, violate 16 C.F.R. § 465.2(a)(1) and therefore are deceptive or unfair acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT VI

Purchasing Fake or False Consumer Reviews

158. In numerous instances, through the means described in Paragraphs 115–118 and 123–124, Defendants have purchased a consumer review about Defendants or one of the services Defendants sell, which Defendants knew or should have known materially misrepresented, expressly or by implication, that the reviewer exists or that the reviewer used or otherwise had experience with Defendants’ services.

159. Therefore, Defendants’ acts or practices, as described in Paragraph 158, violate 16 C.F.R. § 465.2(b)(1)–(2) and therefore are deceptive or unfair acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

CONSUMER INJURY

160. Consumers are suffering, have suffered, and will continue to suffer substantial injury as a result of Defendants’ violations of the FTC Act, the TSR, the GLB Act, and the Reviews and Testimonials Rule. Absent injunctive relief by this Court, Defendants are likely to continue to injure consumers and harm the public interest.

PRAYER FOR RELIEF

Wherefore, the FTC requests that the Court:

- A. Enter a permanent injunction to prevent future violations of the FTC Act, the TSR, the GLB Act, and the Reviews and Testimonials Rule;
- B. Grant preliminary injunctive and ancillary relief as may be necessary to avert the likelihood of consumer injury during the pendency of this action and to preserve the possibility of effective final relief, including temporary and preliminary injunctions, and an order freezing assets;

- C. Award monetary and other relief within the Court's power to grant; and
- D. Award any additional relief as the Court determines to be just and proper.

Respectfully submitted,

Dated: 10/5/2026



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