

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,)	CASE NO.: 1:20CR440
)	
Plaintiff,)	JUDGE SOLOMON OLIVER, JR.
)	
v.)	
)	
VLADIMIR DUNAEV,)	PLEA AGREEMENT
)	
Defendant.)	

Pursuant to Rule 11(c)(1)(A) and (B) of the Federal Rules of Criminal Procedure, and in consideration of the mutual promises set forth below, the United States Attorney's Office for the Northern District of Ohio (hereinafter "USAO") and the Department of Justice Criminal Division Computer Crime and Intellectual Property Section ("CCIPS"), (jointly, the "Government") by and through their undersigned attorneys, and the defendant, VLADIMIR DUNAEV (hereinafter "Defendant"), agree as follows:

**MAXIMUM PENALTIES AND OTHER
CONSEQUENCES OF PLEADING GUILTY**

1. **Waiver of Constitutional Trial Rights.** Defendant understands that Defendant has the right to plead not guilty and go to trial. At trial, Defendant would be presumed innocent, have the right to trial by jury or, with the consent of the United States, to trial by the Court, the

Defendant's Initials VD

right to the assistance of counsel, the right to confront and cross-examine adverse witnesses and subpoena witnesses to testify for the defense, the right to testify and present evidence, and the right to be protected from compelled self-incrimination. Defendant understands that Defendant has the right to an attorney at every stage of the proceedings and, if necessary, one will be appointed to represent Defendant. Defendant understands that by pleading guilty, Defendant specifically and voluntarily waives each of these trial rights, except the right to counsel.

Defendant understands that a guilty plea is a complete admission of guilt and if the Court accepts the guilty plea, the Court will find Defendant guilty without a trial.

2. **Statutory Penalties.** Defendant understands that the statutory maximum penalties, and minimum penalties if applicable, for the counts to which Defendant agrees to plead guilty are as follows:

Counts	Statute and Description of Offense	Statutory Sentence Per Count
1	Title 18 U.S.C. § 371: Conspiracy to Commit Computer Fraud and Identity Theft	Maximum imprisonment: 5 years
		Maximum Statutory fine: \$ 250,000
		Maximum period of supervised release: 3 years
		Special assessment: \$100
2	Title 18 U.S.C. § 1349: Conspiracy to Commit Wire Fraud and Bank Fraud	Maximum imprisonment: 30 years
		Maximum Statutory fine: \$ 1,000,000
		Maximum period of supervised release: 3 years
		Special assessment: \$100

3. **Minimum Sentence Must Include Imprisonment.** The sentence for Count Two, Conspiracy to Commit Wire and Bank Fraud may not be satisfied by a term of probation and must include some period of imprisonment.

4. **Special Assessment.** As set forth above, Defendant will be required to pay a mandatory special assessment of \$100 for each count of conviction, for a total of \$200, due immediately upon sentencing.

Defendant's Initials VD

5. **Forfeiture.** Defendant agrees to the destruction by the Federal Bureau of Investigation of all electronic devices that were seized from his person on or about June 2, 2021. Defendant further agrees that such electronic devices were used in the commission of the above-described offenses and that the devices will not be transferred or returned to Defendant. Particularly, Defendant affirms that he is the owner of, and consents to the destruction of, all such electronic devices - which include, but are not limited to, the following:

- a.) OnePlus One A0001 cellular phone; TD-LTE ID# 2014CP1410
- b.) DEXP Achilles G118 laptop, product code: CLV-650-CFHD, s/n: VDK33869166, barcode #: NKW650SC0005K03488
- c.) 1GB Transcend memory card, model: MMC mobile, s/n: 2723671578
- d.) 8GB Kingston memory card, model: SD4, s/n: 106691609315
- e.) 32GB Kingston memory card, model: SDC10G2, s/n: 31645-003.A00LF
- f.) SJCAM digital camera, model: SJ5000X

6. **Costs.** The Court may order Defendant to pay the costs of prosecution and sentence, including but not limited to imprisonment, community confinement, home detention, probation, and supervised release.

7. **Restitution.** The Court may order Defendant to pay restitution as a condition of the sentence, probation, and/or supervised release.

8. **Violation of Probation/Supervised Release.** If Defendant violates any term or condition of probation or supervised release, such violation could result in a period of incarceration or other additional penalty as imposed by the Court. In some circumstances, the combined term of imprisonment under the initial sentence and additional period of incarceration could exceed the maximum statutory term.

9. **Immigration Consequences.** Defendant understands that a convicted person who is not a United States citizen may be removed from the United States, denied citizenship and denied admission to the United States in the future. Defendant recognizes that pleading

Defendant's Initials VD

guilty may have negative consequences with respect to Defendant's immigration status if Defendant is not a citizen of the United States. Under federal law, a broad range of crimes are removable offenses, including the offenses to which Defendant is pleading guilty. Indeed, because Defendant is pleading guilty to 18 USC §1349, removal is presumptively mandatory. Removal and other immigration consequences are the subject of a separate proceeding, however, and Defendant understands that no one, including Defendant's attorney or the Court, can predict to a certainty the effect of Defendant's conviction on Defendant's immigration status. Defendant nevertheless affirms that Defendant wants to plead guilty regardless of any immigration consequences that Defendant's plea may entail, even if the consequence is Defendant's automatic removal from the United States.

10. **Passport Consequences.** Defendant understands that as a result of a conviction, any United States passport in Defendant's name may be denied, revoked, or limited pursuant to Title 26, § 7345 of the United States Code.

PLEAS AND OTHER CHARGES

11. **Agreement to Plead Guilty.** Defendant agrees to plead guilty to Counts 1 and 2 in this case.

12. **Dismissal of Counts.** Upon sentencing, the Government will move to dismiss the charges against Defendant in Counts 3-47 of the Indictment in this case.

13. **Agreement Not to Bring Certain Other Charges.** The Government will not bring any other criminal charges against Defendant for conduct disclosed to the Government by Defendant during the investigation of the Defendant's case.

ELEMENTS OF THE OFFENSE

14. The elements of the offense to which Defendant will plead guilty are:

Title 18 U.S.C. § 371: Conspiracy to Commit Computer Fraud
--

Defendant's Initials VD

1: Two or more persons conspired, or agreed, to commit the crime alleged in the indictment;
2: The Defendant knowingly and voluntarily joined the conspiracy; and
3: At some point during the existence of the agreement or conspiracy, at least one of its members performed an overt act for the purpose of advancing or helping the conspiracy.
Title 18 U.S.C. § 1349: Conspiracy to Commit Wire Fraud
1: Two or more persons conspired, or agreed, to commit the crime alleged in the indictment;
2: The Defendant knowingly and voluntarily joined the conspiracy.
3: At some point during the existence of the agreement or conspiracy, at least one of its members performed an overt act for the purpose of advancing or helping the conspiracy.

SENTENCING STIPULATIONS AND AGREEMENTS

15. **Sentencing Guidelines.** Defendant understands that sentencing rests within the discretion of the Court; that federal sentencing law requires the Court to impose a sentence which is sufficient, but not greater than necessary, to comply with the purposes of 18 U.S.C. § 3553(a), and that the Court must consider among other factors the advisory United States Sentencing Guidelines in effect at the time of sentencing and that in determining the sentence, the Court may depart or vary from the advisory guideline range.

16. **Presentence Report.** Defendant understands that the advisory guideline range will be determined by the Court at the time of sentencing, after a presentence report has been prepared by the U.S. Probation Office and reviewed by the parties. Defendant further understands that the Government may provide to the U.S. Probation Office all known information regarding Defendant's conduct subject to its limited use under U.S.S.G. § 1B1.8 and except as protected under the proffer agreement if any.

17. **Joint Recommendation to Use the Advisory Sentencing Guidelines Computation.** After considering the factors in 18 U.S.C. §3553(a), the parties agree to recommend that the Court impose a sentence within the range and of the kind specified pursuant to the Advisory Sentencing Guidelines in accordance with the computations and stipulations set

Defendant's Initials VD

forth below. Neither party will recommend or suggest in any way that a departure or variance is appropriate, either regarding range or the kind of sentence imposed.

18. **Sentencing Recommendations Not Binding on the Court.** Defendant understands that the recommendations of the parties will not be binding upon the Court, that the Court alone will decide the advisory guideline range under the Sentencing Guidelines, whether there is any basis to depart from that range or impose a sentence outside the advisory guideline range, and what sentence to impose. Defendant further understands that once the Court has accepted Defendant's guilty plea, Defendant will not have the right to withdraw such a plea if the Court does not accept any sentencing recommendations made on Defendant's behalf or if Defendant is otherwise dissatisfied with the sentence.

19. **Allocution.** Defendant understands and agrees that the Government reserves the opportunity to speak at Defendant's sentencing. The Government agrees that Defendant reserves the right of allocution at sentencing.

20. **Stipulated Guideline Computation.** The parties agree that the following calculation, using the current advisory Sentencing Guidelines Manual, represents the correct computation of the applicable offense level:

Defendant's Initials VP

Count 1: Conspiracy to Commit Computer Fraud, 18 USC § 371		
Base offense level	6	§ 2B1.1(a)(2)
Loss: 3,500,000 to 9,000,000	18	§ 2B1.1(b)(1)(J)
Ten or more victims	2	§ 2B1.1 (b)(2)(A)
Relocation of scheme overseas:	2	§ 2B1.1(b)(10)(B)
Use of Special Skill:	2	§ 3B1.3
Subtotal	30	
Count 2: Conspiracy to Commit Wire Fraud, 18 USC § 1349		
Base offense level	7	§ 2B1.1(a)(1)
Loss: 3,500,000 to 9,000,000	18	§ 2B1.1(b)(1)(J)
Ten or more victims	2	§ 2B1.1 (b)(2)(A)
Relocation of scheme overseas:	2	§ 2B1.1(b)(10)(B)
Use of Special Skill:	2	§ 3B1.3
Subtotal	31	

21. **Acceptance of Responsibility.** The Government has no reason to believe at this time that Defendant has not clearly and affirmatively accepted personal responsibility for Defendant's criminal conduct. The Government agrees to recommend a three (3) level reduction for acceptance of responsibility under U.S.S.G. § 3E1.1(a) and (b), provided Defendant's conduct continues to reflect Defendant's acceptance of responsibility. Defendant understands it will be up to the Court at the time of sentencing to determine whether a reduction for acceptance of responsibility is appropriate.

22. **Criminal History Category.** The parties have no agreement about the Criminal History Category applicable in this case. Defendant understands that the Criminal History Category will be determined by the Court after the completion of a Pre-Sentence Investigation by the U.S. Probation Office.

23. **Adjustment for Certain Zero-Point Offenders.** The parties recognize that U.S.S.G. § 4C1.1(a) could result in a further 2-level reduction in Defendant's offense level if, among other things, the Defendant is determined to have zero Criminal History points. The USAO agrees to recommend the application of this 2-level reduction if the final Pre-Sentence

Defendant's Initials VD

Investigation Report determines Defendant has zero Criminal History points and is not otherwise disqualified from the application of U.S.S.G. § 4C1.1(a). Defendant agrees that the Court's decision on the application of U.S.S.G. § 4C1.1(a) shall be final, and treated as part of "the sentencing stipulations and computations in this agreement" in the following section ("Waiver of Appeal and Post-Conviction Attack").

WAIVER OF APPEAL AND POST-CONVICTION ATTACK

24. Defendant acknowledges having been advised by counsel of Defendant's rights, in limited circumstances, to appeal the conviction or sentence in this case, including the appeal right conferred by 18 U.S.C. § 3742, and to challenge the conviction or sentence collaterally through a post-conviction proceeding, including a proceeding under 28 U.S.C. § 2255. Defendant expressly and voluntarily waives those rights, except as specifically reserved below. Defendant reserves the right to appeal: (a) any punishment in excess of the statutory maximum; or (b) any sentence to the extent it exceeds the maximum of the sentencing imprisonment range determined under the advisory Sentencing Guidelines in accordance with the sentencing stipulations and computations in this agreement, using the Criminal History Category found applicable by the Court. Nothing in this paragraph shall act as a bar to Defendant perfecting any legal remedies Defendant may otherwise have on appeal or collateral attack with respect to claims of ineffective assistance of counsel or prosecutorial misconduct.

WAIVER OF STATUTE OF LIMITATIONS

25. Defendant waives all defenses based on the statute of limitations with respect to any prosecution that is not already time-barred by the applicable statute of limitation on the date of Defendant's signing of this agreement and that is commenced within one year after any of the following events: (1) Defendant fails to plead guilty at the plea proceeding or the Court refuses to accept a guilty plea by Defendant pursuant to this agreement; (2) the Court permits Defendant

Defendant's Initials VD

to withdraw a guilty plea entered pursuant to this agreement or otherwise vacates such a guilty plea; or (3) the conviction obtained pursuant to this agreement is vacated, overturned, or otherwise set aside. Defendant understands the waiver of the statute of limitations is effective immediately upon Defendant's signing of this agreement and is not conditioned upon the approval of this agreement by the Court.

FACTUAL BASIS AND RELEVANT CONDUCT

26. Defendant agrees that the following summary fairly and accurately sets forth Defendant's offense conduct and a factual basis for the guilty plea. Defendant further agrees that the facts set forth in the summary are true and could be established beyond a reasonable doubt if the case were to proceed to trial:

- a. From at least on or about June of 2016 and continuing through on or about June 2, 2021, DUNAEV performed a variety of developer functions in support of the Trickbot malware and the network managing the malware's execution.
- b. The Trickbot Group was a transnational organized cybercrime network that developed and used a suite of malware named Trickbot to deploy ransomware and steal money and personal and confidential information from unsuspecting victims, including businesses and their financial institutions located in the United States, United Kingdom, Australia, Belgium, Canada, Germany, India, Italy, Mexico, Spain, and Russia.
- c. Trickbot Group conspirators specialized in tasks to combine and work to: (a) infect victims' computers with Trickbot malware designed to capture victims' online banking login credentials; (b) obtain and harvest other personal identification information, including credit cards, emails, passwords, dates of birth, social security numbers, and addresses; (c) infect other computers on the victims' network; (d) use captured login credentials to fraudulently gain unauthorized access to victims' online

Defendant's Initials VD

bank accounts at financial institutions; (e) steal funds from victims' bank accounts and launder those funds using U.S. and foreign beneficiary bank accounts provided and controlled by Trickbot Conspirators; and (f) install ransomware on victim computers.

d. Trickbot was designed to evade detection by anti-virus software and other protective measures employed by victims and was generally spread through phishing and spear phishing email campaigns. Once installed on a victim computer, Trickbot, in part, used web injects and keystroke logging to obtain and harvest online banking credentials from infected victim computers. Defendants then used these credentials to gain unauthorized access to victims' bank accounts and then transferred and attempted to transfer funds from the victims' accounts to accounts controlled by Defendants. Later versions of Trickbot were adapted to facilitate the installation and use of ransomware. During the entire lifespan of the Trickbot Group, millions of computers worldwide were infected.

e. In the United States, Trickbot primarily targeted victim computers belonging to U.S. businesses, entities, and individuals, including those within the Northern District of Ohio.

f. In order to perpetrate their criminal schemes, Defendants used a network of co-conspirators, including DUNAEV, who provided specialized services and technical abilities in furtherance of the criminal scheme. The specialized skills and services included soliciting and recruiting malware developers; purchasing and managing servers from which to test, deploy, and operate the Trickbot malware; encrypting the malware to avoid detection by anti-virus software; engaging in spamming, phishing, and spear-

Defendant's Initials VD

phishing campaigns against potential victims; and coordinating the receipt and laundering of funds from the victims to Defendants and others.

g. For instance, DUNAEV developed browser modifications for several widely used open-source browsers, such as FireFox and Chrome, using open-source codebases for each browser called FireFox Nightly and Chromium. These modifications facilitated and enhanced the remote access obtained by Trickbot by allowing actors to steal passwords, credentials, and other stored information. DUNAEV also developed malicious tools that aided in credential harvesting and datamining from infected computers.

h. Additionally, DUNAEV developed a program code which was used to conceal the Trickbot malware from being detected by legitimate security software.

i. DUNAEV was recruited and posted projects on a work-sharing service used by the Trickbot Group called GitLab. Below is a chart detailing the dates and subjects of DUNAEV's posting work on GitLab for use by the Trickbot Group:

Email used	Date	Notes about work performed
Dunaev666@gmail.com	August 2, 2016	"1"
Dunaev666@gmail.com	August 4, 2016	"v0.11 fixed buffer overflow bug (unexpected sizes)"
Dunaev666@gmail.com	October 3, 2016	"v0.20 - storage grabbing added"
Dunaev666@gmail.com	October 5, 2016	"v0.21 - fixed dllhost crash"
Dunaev666@gmail.com	October 17, 2016	"v0.30 - public suffix list support added"
Dunaev666@gmail.com	October 21, 2016	"v0.31 - IP domain fixed - ie registry path fix - esentutl repair problem fix (partial retries added)"
Dunaev666@gmail.com	October 26, 2016	"v0.32 - registry redirect 64/32 platform fixed - domstore datalow path added - google busy history fixed"
Dunaev666@gmail.com	October 27, 2016	"v0.33 - ie 8,9 DOMStore not found after cleaning history fix"
Dunaev666@gmail.com	November 11, 2016	"v0.331 - small fixes"
Dunaev666@gmail.com	December 10, 2016	"v0.34 - restricted (lite) version added for managing lso"
Dunaev666@gmail.com	February 14, 2017	"v0.341 - Microsoft compiler fixes - small x64/x86 fixes"
Dunaev666@gmail.com	February 16, 2017	"v0.342 - small fixes"

Defendant's Initials VD

Dunaev666@gmail.com	March 11, 2017	"v0.343 - map exceptions fixes"
Dunaev666@gmail.com	March 12, 2017	"v0.35 - SQLite version display added"
Dunaev666@gmail.com	March 27, 2017	"v0.36 - windows waitForReadyRead() fix"
Dunaev666@gmail.com	May 18, 2017	"v0.361 - grablso now dynamic"
Dunaev666@gmail.com	May 24, 2017	"v0.40 - ic depricated stuff grabbing added - optimizations"
Dunaev666@gmail.com	June 7, 2017	"v0.401 - fixes (linux version)"
Dunaev666@gmail.com	November 21, 2018	"chrome leveldb added"
Dunaev666@gmail.com	November 21, 2018	"updated public suffix"
Dunaev666@gmail.com	December 3, 2018	"v0.5 - leveldb support added for chrome localStorage - grabber lib added for launcher profile exchange - new fields : navigator.deviceMemory, timezone.txt - browser type added in conf.type"
Dunaev666@gmail.com	December 14, 2018	"v0.51 - confdata save to qbytearray added"

j. In furtherance of the scheme to defraud by the Trickbot Group, and through the use of the Trickbot Malware which used the computer utilities developed by DUNAIEV, between on or about October 3, 2018 and continuing to on or about February 6, 2021, over ten victims in the Northern District of Ohio and elsewhere, were defrauded of in excess of 3.4 million dollars, which was moved by wire transmissions by members of the Trickbot Group overseas to avoid detection by authorities and for their personal gain.

27. Defendant acknowledges that the above summary of Defendant's conduct does not set forth each and every fact that the Government could prove at trial, nor does it encompass all of the acts which Defendant committed in furtherance of the offenses to which Defendant is pleading guilty.

RESTITUTION

28. **Restitution.** Defendant agrees to make full restitution as ordered by the Court pursuant to 18 U.S.C. § 3663, on a joint and several basis, payable immediately on such terms and conditions as the Court may impose, for the losses caused by Defendant's relevant conduct in

Defendant's Initials VD

this case, as defined under Guideline § 1B1.3. Defendant agrees not to seek the discharge of any restitution obligation, in whole or in part, in any present or future bankruptcy proceeding.

Defendant understands that pursuant to 18 U.S.C. § 3664, the Court shall order the U.S. Probation Office to prepare a report containing information sufficient for the Court to fashion a restitution order. In preparing that report, the U.S. Probation Office may solicit the views of the Government, Defendant, and any victim. Defendant understands that victims have the right to present their position on restitution directly to the Court at the time of sentencing.

OTHER PROVISIONS

29. **Financial Statement.** Defendant agrees upon request to submit to the Government, prior to the date of sentencing, a complete and accurate financial statement on a Financial Statement of Debtor Form to be provided by the Government.

30. **The Parties are Free to Advise the Court about Matters Not Expressly Addressed.** This agreement is silent about all aspects of the determination of sentence not expressly addressed herein, and the parties are free to advise the Court of facts and to make recommendations to the Court with respect to all aspects of sentencing not agreed to herein.

31. **Consequences of Breaching the Plea Agreement.** Defendant understands that if Defendant breaches any promise in this agreement, commits additional crimes, obstructs justice, attempts to withdraw Defendant's guilty plea, or if Defendant's guilty plea is rejected by the Court or is vacated or set aside, the Government will be released from all of its obligations under this agreement and may institute or maintain any charges and make any recommendations with respect to sentencing that otherwise would be prohibited under the terms of the agreement. Defendant understands, however, that a breach of the agreement by Defendant will not entitle Defendant to withdraw, vacate, or set aside Defendant's guilty plea or conviction. Defendant

Defendant's Initials VD

understands that the Government has the right to use any statement Defendant gives under oath in a prosecution for perjury or false statement.

32. **Agreement not Binding on other Jurisdictions and Agencies.** Defendant understands that this plea agreement is binding only on the United States Attorney's Office for the Northern District of Ohio. It does not bind any other United States Attorney, any other federal agency, or any state or local government.

33. **Defendant is Satisfied with Assistance of Counsel.** Defendant makes the following truthful statements: I have discussed this case and this plea agreement in detail with my attorney who has advised me of my Constitutional and other trial and appeal rights, the nature of the charges, the elements of the offenses the United States would have to prove at trial, the evidence the United States would present at such trial, possible defenses, the advisory Sentencing Guidelines and other aspects of sentencing, potential losses of civil rights and privileges, and other potential consequences of pleading guilty in this case. I have had sufficient time and opportunity to discuss all aspects of the case in detail with my attorney and have told my attorney everything I know about the charges, any defenses I may have to the charges, and all personal and financial circumstances in possible mitigation of sentence. I am satisfied with the legal services and advice provided to me by my attorney.

34. **Agreement Is Complete and Voluntarily Entered.** Defendant and Defendant's undersigned attorney state that this agreement, including any addendums discussed in open court and on the record at the time of the change of plea (if any), is the entire agreement between Defendant and the Government and that no other promises or inducements have been made, directly or indirectly, by any agent or representative of the United States government concerning any plea to be entered in this case. In particular, no promises or agreements have been made with

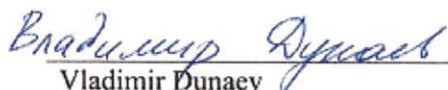
Defendant's Initials VD

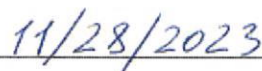
respect to any actual or prospective civil or administrative proceedings or actions involving Defendant, except as expressly stated herein. In addition, Defendant states that no person has threatened or coerced Defendant to do or to refrain from doing anything in connection with this case, including Defendant's decision to enter a guilty plea. Finally, Defendant acknowledges that this agreement cannot be modified unless in writing and subject to approval by the Court.

Defendant's Initials VD

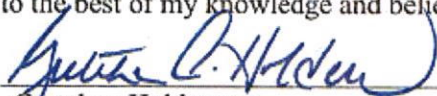
SIGNATURES

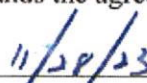
Defendant: I have read (or have had read to me) this entire plea agreement and have discussed it with my attorney. I have initialed each page of the agreement to signify that I understand and approve the provisions on that page. I am entering this agreement voluntarily and of my own free will. No threats have been made to me, nor am I under the influence of anything that could impair my ability to understand this agreement.


Vladimir Dunaev
Defendant

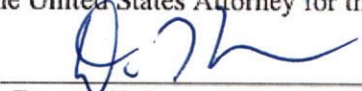

Date

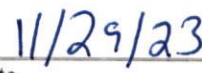
Defense Counsel: I have read this plea agreement and concur in Defendant pleading in accordance with terms of the agreement. I have explained this plea agreement to Defendant, and to the best of my knowledge and belief, Defendant understands the agreement.


Gretchen Holderman
Counsel for Defendant


Date

United States Attorney's Office: I accept and agree to this plea agreement on behalf of the United States Attorney for the Northern District of Ohio.


Duncan T. Brown (NY: 3982931)
Assistant United States Attorney
801 West Superior Avenue; Suite 400
Cleveland, OH 44113
Email: Duncan.Brown@usdoj.gov


Date

Defendant's Initials VD

**Computer Crime and Intellectual Property Section of the Department of Justice,
Criminal Division:** I accept and agree to this plea agreement on behalf of the Computer
Crime and Intellectual Property Section of the Department of Justice, Criminal Division.

/s/Candina S. Heath

Candina S. Heath (TX: 09347450)
Senior Counsel
1301 New York NW Ave
Washington, DC 20530
Email: Candina.Heath2@usdoj.gov

11/29/2023

~~11/29/2023~~

Date

APPROVED:

SOLOMON OLIVER, JR.

United States District Court Judge

Date

Defendant's Initials VD