UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

UNITED STATES OF AMERICA

v. Case No. 8:24-cr-00068-KKM-TGW

TIMOTHY BURKE

UNITED STATES' MOTION FOR ENTRY OF PROTECTIVE ORDER AND INCORPORATED MEMORANDUM IN SUPPORT

Pursuant to Rule 16(d)(1) of the Federal Rules of Criminal Procedure and 18 U.S.C. § 3771(a) and (d), the United States of America requests that this Court enter a protective order in this case limiting the dissemination of certain discoverable materials, namely materials that contain personally identifying information ("PII"), intellectual property of others (*e.g.*, proprietary information, trade secrets, and copyrighted material), and/or are contraband, secured during the investigation leading to the indictment in this case. The United States submits the following in support of a finding of good cause for the requested relief:

I. The Charges

A. The Charges Against Burke

On February 15, 2024, a federal grand jury sitting in the Middle District of Florida returned a fourteen-count indictment against defendant Timothy Burke, charging him in Count One with engaging in a conspiracy from in or around February 2022, and continuing through May 2023, in violation of 18 U.S.C. § 371; in

Counts Two through Seven with intentionally accessing a protected computer without authorization, in violation of 18 U.S.C. § 1030(a)(2)(C); in Counts Eight through Twelve with intentional interception of a wire, oral, or electronic communication, in violation of 18 U.S.C. § 2511(1)(a); and in Counts Thirteen and Fourteen with intentionally disclosing an illegally intercepted wire, oral, or electronic communication, in violation of 18 U.S.C. § 2511(1)(c). Doc. 1. The indictment also includes forfeiture allegations that list twenty items subject to forfeiture that were seized from Burke's residence on May 8, 2023.[1] *Id.*

The indictment identifies via anonymizations for privacy some of the entities harmed by the conduct charged, namely the NSL, StreamCo, Network #1, and Network #2 (the "Victim Entities"). *Id.* at Count One, ¶¶ 5-16. As alleged in Count One, Section C,[2] Burke and "Conspirator 2"—now identified as Marco Gaudino—utilized the Internet to secure credentials (usernames and passwords), which had been issued to others with whom Burke and Gaudino had no affiliation, and from whom neither Burke nor Gaudino had received any authorization to possess or use.[3] Doc. 1 at Count One, ¶¶ 22.a.-c. Burke and Gaudino then repeatedly utilized the compromised credentials to gain unauthorized access to Victim Entities' protected

[1] Burke has had an initial appearance, has been released on conditions set by the Court, and has been arraigned.

[2] The Manner and Means of the Conspiracy section.

[3] *See, e.g.,* Count One, Section D, at ¶¶ 23.a.1-2., 23.d.1-2.

computers,[4] and then scoured those computers for desirable items and information, which they stole by producing unauthorized copies of the (nonpublic) items and information for their own use.[5] *Id.* at ¶¶ 22.d.-f.

As to Victim Entity StreamCo, the indictment alleges that Burke and Gaudino stole information from StreamCo-Net,[6] a StreamCo service accessible to customers via a secure password-protected website, used that stolen information to unlawfully intercept the contents of video communications as they were being transmitted across the StreamCo-Net by its broadcaster-customers, and downloaded and saved the unlawfully intercepted video communications to the conspirators' respective computers.[7] *Id.* at 22.g.-h. The indictment further charges that Burke and Gaudino exchanged direct messages throughout the conspiracy, some of which concerned their coordinated efforts to disclose certain unlawfully intercepted video communications.[8] *Id.* at 22.i.-l. The indictment against Burke then charges in Counts Two through Fourteen discrete substantive criminal acts engaged in by Burke and/or Gaudino during the period of the conspiracy.

---

[4] A "protected computer" is defined in Count One, ¶ 18. Doc. 1.

[5] *See, e.g.,* Count One, Section D, at ¶¶ 23.b.1-4., 23.c.1-3, 23.e.1-7, and 23.h.1-5.

[6] *See, e.g.,* Count One, Section D, at ¶¶ 23.h.1-5.

[7] *See, e.g.,* Count One, Section D, at ¶¶ 23.i.1-5.

[8] *See, e.g.,* Count One, Section D, at ¶¶ 23.j.1-2.

B. Marco Gaudino's Information and Plea Agreement

On April 12, 2024, the United States filed a one-count information charging Burke's co-conspirator, Marco Gaudino, in Case No. 8:24-cr-00165-CEH-SPF (the "Gaudino Case"), for his role in the conspiracy charged against Burke in this case. Gaudino Case, Doc. 1. One week later, the United States filed a fully executed plea agreement between the United States and Gaudino, in which Gaudino admitted certain facts regarding the charged conspiracy. Gaudino Case, Doc. 9. Gaudino then appeared in court later that same day and confirmed under oath the accuracy of the Factual Basis section of his plea agreement and his guilt in the charged conspiracy. Gaudino Case, Doc. 15. Notably, Gaudino acknowledged and confirmed multiple acts involving himself and Burke, including their participation in direct-message exchanges about securing and using compromised credentials belonging to others to unlawfully access protected computers without authorization, including one exchange during which the conspirators shared nine additional credential sets associated with a protected computer owned by a Victim Entity identified within the Factual Basis as "TSN," or a sports network. Gaudino Case, Doc. 9 at 24 and 27-28.

Gaudino specifically confirmed: "he was not employed by or otherwise associated with the NSL, TSN, StreamCo, StreamCo-Net, NW-1, or NW-2, and that he did not have authorization from any of the entities or associated credential holders to utilize the [identified] credentials to access the entities' [listed] computers." *Id.* at 30. As to how Gaudino acquired certain compromised credentials utilized by the conspirators, Gaudino acknowledged that:

> prior to 2020, he unlawfully obtained compromised credentials from an Internet website dealing unlawfully in such credentials, which enabled him to gain unauthorized access to a protected computer hosting an NSL archive site. There, GAUDINO found, amongst other electronic items and information, a second set of credentials that enabled him to gain unauthorized access to a second protected computer, namely the NSL FTP server located at ftp://ftp01.NSL.com, referred to [in GAUDINO's information and plea agreement], which GAUDINO shared with BURKE. Further, GAUDINO originally acquired the compromised NW-2 credentials [. . .] that were used by GAUDINO and BURKE to gain unauthorized access to a protected computer, namely the StreamCo-Net, from an online acquaintance who GAUDINO understood was not authorized to possess or utilize such credentials.

Id. at 30-31.

II. Discovery

A. Discoverable Material Requiring Safeguards

On April 2, 2024, this Court entered the *Pretrial Discovery Order and Notice of Trial and Status Conference* (the "Pretrial Discovery Order"), regulating the discovery proceedings in this case. Thereafter, on April 12th, the United States hosted the Burke defense team at the Tampa United States' Attorney's Office for a Rule 16.1 Pretrial Discovery Conference (the "Discovery Conference"). During that Discovery Conference, the United States identified and generally described the broad categories of discoverable items, data, and information that potentially could be deemed material to the preparation of the defense or that were obtained from or belonged to defendant Burke or are intended for use by the United States in its case-in-chief, as defined in Rule 16(a)(1)(E).

The United States elaborated that the available discoverable material is voluminous, exceeding more than approximately 50 terabytes, and is composed of

all manner of documents, electronic worksheets, data (personal, financial, and business related), communications, images, and video streams.[9] The United States further explained to the defense team that certain discoverable items contain PII, intellectual property of others (*e.g.*, trade secrets and copyrighted material), and/or contraband,[10] and require safeguards to protect the items from public disclosure.[11]

i. PII and Business Customer Identifying Data. Some of the information secured during the investigation is properly considered PII or business customer identifying data. In that regard, said information includes names, birthdates, financial and personal account numbers, home addresses, and other information falling under the protections of Fed. R. Crim. P. 49.1 and other related rules and policies. By way of example, it was necessary for the investigative team to secure PII and other related information about individuals whose presence was detected in certain Victim Entity online platform logs only by IP address and/or a login credential in order to identify said individuals and to determine whether those individuals were accessing a particular platform at a particular time with or without authorization.[12] It was further necessary to secure certain information from one or

[9] 50 terabytes of data is roughly equivalent to 50,000 gigabytes of data.

[10] The United States recognizes that the Burke defense team does not concur with or approve of the United States' description of any property secured from Burke as "contraband."

[11] Some of the discoverable items are also properly considered to be instrumentalities used during and in furtherance of the charged conduct.

[12] The offered example illustrates only one circumstance in a lengthy, complex investigation that has secured a voluminous amount of available discoverable material, most of which is maintained in electronic format and impractical to redact.

more Victim Entities that include sensitive, nonpublic customer account information to determine the reach and impact of the charged criminal conduct.

ii. Intellectual Property. Victim Entities identified in the indictment have produced information to the United States during the investigation that the businesses have identified as nonpublic proprietary information and/or trade secrets,[13] the public disclosure of which would have adverse impacts on the businesses' competitive advantage within their respective marketplaces. As just one example, one Victim Entity has expressed concern to the United States that the material produced to the investigation by the Victim Entity contains PII and information about the Victim Entity's internal business processes and customers, including customer-account information and related internal sales information.

[13] While this case does not presently include any charges under 18 U.S.C. Chapter 90 (Protection of Trade Secrets), a useful definition of trade secrets can be found at 18 U.S.C. § 1839(3)—

> [T]he term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if-
>
> (A) the owner thereof has taken reasonable measures to keep such information secret; and
>
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information[.]

iii. Contraband. The United States is in possession of certain discoverable materials that were seized during the execution of court-authorized search warrants, including a search conducted at the defendant's residence on May 8, 2023. The United States has explained to the defense team that some of these materials contain what the United States has identified as "contraband," or fruits of the alleged criminal conduct at issue in this case.[14] For example, the United States is in possession of approximately 3,079 folders/files (approximately 1.6 TB of data) seized from Burke's computer system that, per the United States' investigation, were downloaded by Burke from the NSL FTP server located at ftp://ftp01.[NSL].com—referred to in Count One of the indictment (*see* ¶¶ A.5.-6. and D.23.a-c.), and in Counts Two and Three—after accessing that protected computer using the compromised credential supplied to Burke by co-conspirator Gaudino. Doc. 1.

The United States is likewise in possession of information found on Burke's computer system that was stolen from a StreamCo-Net computer, which Burke had accessed using other compromised credentials, as alleged in Count One (*see* ¶¶ D.23.d-h) and in Counts Two through Seven. *Id*. Relatedly, the investigative team located on Burke's system approximately 1,073 files (approximately 87.15 GB) that contain all or part of what appears to be intercepted and stolen wire communication streams of NW-1, NW-2, and other victim entities, as charged in

[14] The United States has already returned to Burke copies of all folders and files secured from Burke's residence on May 8, 2023, which are not considered contraband. The return of this material was accounted for in related litigation, namely *Tampa Bay Times v. United States*, Case No. 8:23-cr-00014-WFJ-SPF (the "TBT Case"). *See, e.g*, TBT Case Docs. 37, 47, 47-1, and 49."

Count One and in Counts Eight through Twelve.[15, 16] *Id.* Affected Victim Entities have explained to the United States that video streams created by or for said Victim Entities (and others) but stolen and downloaded by the conspirators are subject to copyright protection and should be safeguarded.

In response to the United States' explanations during the April 12th Discovery Conference about the discoverable material available, the Burke defense team expressed, in part, its desire to secure a forensically sound copy of Burke's computer system and other seized devices, as the system and devices existed at Burke's residence on May 8, 2023, for use in the defense team's investigation and trial preparation efforts. To that end, the United States made clear that it is amenable to working cooperatively with the defense team to reach an agreed-upon procedure, memorialized in writing and/or court order, as necessary, that will satisfy the defense team's request while maintaining the necessary and appropriate safeguards over the discoverable items which contain PII, intellectual property of others (*e.g.*, trade secrets and copyrighted material), and/or contraband.

B. Ongoing Discovery Process

Following the initial Discovery Conference, the United States, on April 18, 2024, sent its initial discovery letter to the Burke defense team that again generally

[15] The provided examples should not be understood as representing the entirety of the contraband files in the United States' possession.

[16] Like items requiring safeguarding have been identified on Gaudino's computer system and are also available as discoverable material.

described the available discoverable material and repeated the United States' earlier expressed concerns regarding the need to protect a subset of the material from public disclosure. The United States attached to its discovery letter an Attachment A that itemized some of the discoverable material and identified certain items that, along with the available search warrant materials, the United States has identified as containing PII, intellectual property of others, and/or contraband (hereinafter, "Covered Materials").[17] The United States explained in its letter that the United States was prepared to transmit to the defense team via USAFX all information associated with the items listed in Attachment A that were not identified as Covered Materials requiring safeguards. The United States has now made two productions to the defense team of discoverable items that do not contain the identified Covered Materials.

As to the subset of Covered Materials requiring protection from public disclosure, the United States, in its discovery letter, notified the defense team that the Covered Materials are available for inspection and review at the Tampa FBI office. The United States further explained that, as discussed during the April 12th Discovery Conference, the United States remained amenable to working cooperatively with the defense team to reach an agreed-upon procedure by which the defense team has direct possession and access to Covered Materials, including a forensically sound copy of Burke's system and other seized devices (secured via

[17] The following day, the United States sent a letter that amended the Attachment A.

warrants), provided the appropriate safeguards were established. To facilitate that result, the United States proposed that an agreement be reached between the parties that included the following features and guardrails:

- A copy of the Covered Material (including the identified contraband) will be made available to the defense team for its use in investigating and preparing for trial;
- The Covered Material made available by the United States to the defense team in this case shall not be reproduced or disseminated to persons not a party to, or involved, in this case;
- Defense counsel for Burke will not allow Burke unsupervised access to the Covered Material; and
- Any person who receives a copy of any document or information subject to the agreed-upon procedure or court order in the investigation or preparation of this case shall not reproduce or disseminate said document or information except as provided for in the procedure or order.

The United States then prepared and submitted to the Burke defense team on Friday, April 26, 2024, a copy of a proposed motion for protective order and a protective order, substantially similar to the proposed order submitted with this motion. The United States has now been informed by the Burke defense team that it "decline[s] to agree to any restrictions on the use of materials provided in discovery other than those in Fed. R. Crim. [P.] 49 and local rule 3:11." The defense team further articulated its position that all information seized by the United States from

Burke had been obtained lawfully by Burke and that he retained the right to publish it.[18]

MEMORANDUM IN SUPPORT

Fed. R. Crim. P. 16(d)(1), entitled "Protective and Modifying Orders," expressly authorizes this Court to issue protective orders: "At any time the court may, for good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief." Moreover, Rule 16(d)(1) allows a court to review a party's statement *ex parte* in support of establishing good cause for a requested protective order.[19] A protective order that limits a criminal defendant's treatment of discoverable materials is therefore an appropriate use of the Court's discretion. *Alderman v. United States*, 394 U.S. 165, 185 (1969) ("[T]he trial court can and should, where appropriate, place a defendant and his counsel under enforceable orders against unwarranted disclosure of the materials which they may be entitled to inspect."); *see also United States v. Campa*, 529 F.3d 980, 995 (11th Cir. 2008) (recognizing "[t]he broad authority of the district court to regulate discovery" in a criminal case); *and see United States v. Hsu*, 155 F.3d 189, 197 (3rd Cir. 1998) (presumption in favor of protecting trade secrets, in that doing so encourages

[18] Of course, given the pending indictment against Burke, that position is without merit, regardless of whether one accepts Burke's asserted status as a news journalist. As recognized by the Supreme Court in *Branzburg v. Hayes*, 408 U.S. 665, 691 (1972), it would be "frivolous" to assert—much less hold—that a reporter or his sources would have a "license . . . to violate valid criminal laws."

[19] The United States is amenable to producing additional information, including specific examples of Covered Materials, to this Court *ex parte*, should the Court so desire.

enforcement actions by protecting owners of such information who might otherwise be reluctant to cooperate in prosecutions out of fear that doing so would expose trade secrets to public view).[20]

Here, a federal grand jury has found probable cause and returned an indictment against defendant Burke, charging Burke with conspiracy and substantive crimes relating to his unlawful agreement with Gaudino to: (1) gain unauthorized access to protected computers of others from which the conspirators stole information, (2) unlawfully intercept the contents of video communications, and (3) disclose the same. Gaudino has entered into a plea agreement with the United States and pleaded guilty for his role in that charged conspiracy.

As explained above, the voluminous discoverable materials in this case include a significant subset of items and information secured during the investigation—via subpoenas, search warrants, and other means—leading to the pertinent indictment that have been identified as containing PII, intellectual property of others, and/or contraband. Information stolen from victim businesses and video communications unlawfully intercepted by Burke and Gaudino are properly considered as contraband, which require safeguards to protect that information and

[20] Indeed, in a case charging a violation of 18 U.S.C. Chapter 90 (Protection of Trade Secrets), a court is directed under 18 U.S.C. § 1835 to: "enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws."

those communications from public disclosure. In addition, the intellectual property of others that has been produced to the United States during the investigation leading to the indictment against Burke (and information charging Gaudino) should likewise be protected, as should PII and business customer identifying data.

The requested entry of a protective order in this case is also appropriate under the Crime Victims' Rights Act, which recognizes that crime victims, such as the Victim Entities referred to in the indictment returned against Burke, have a "right to be reasonably protected from the accused[,]" namely Burke. *See* 18 U.S.C. § 3771(a)(1). Said Victim Entities also have the right "to be treated with fairness and with respect for [their] dignity *and privacy*." 18 U.S.C. § 3771(a)(8) (emphasis added). Congress has therefore specifically directed district courts to "take up and decide any motion asserting a victim's right [under the provision] forthwith[,]" which may be brought by a victim, a victim's lawful representative, or an attorney for the government. 18 U.S.C. § 3771(d)(1) and (3).

Wherefore, the United States requests that this Court enter the proposed protective order, attached hereto as Exhibit 1. Such order will enable the Burke defense team to have direct access to a forensically sound copy of Burke's system and other discoverable materials while maintaining necessary and appropriate safeguards

over discoverable items that contain PII, intellectual property of others, and/or contraband.

Respectfully submitted,

ROGER B. HANDBERG
United States Attorney

By: */s/ Jay G. Trezevant*

Jay G. Trezevant
Assistant United States Attorney
Florida Bar No. 0802093
400 N. Tampa St., Suite 3200
Tampa, Florida 33602-4798
Telephone: (813) 274-6000
Email: jay.trezevant@usdoj.gov

/s/ Adam J. Duso

Adam J. Duso
Assistant United States Attorney
Florida Bar No. 1026003
400 N. Tampa St., Suite 3200
Tampa, Florida 33602-4798
Telephone: (813) 274-6000
Email: adam.duso@usdoj.gov

U.S. v. TIMOTHY BURKE **CASE NO. 8:24-cr-00068-KKM-TGW**

CERTIFICATE OF SERVICE

I hereby certify that on May 6, 2024, I electronically filed the foregoing with the Clerk of the Court by using the CM/ECF system which will send a notice of electronic filing to counsel for the Defendant.

/s/Jay G. Trezevant
Jay G. Trezevant
Assistant United States Attorney