IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

KONNECH, INC.,	§	
	§	
PLAINTIFF,	§	
	§	
v.	§	**CIVIL ACTION NO. 4:22-CV-03096**
	§	
TRUE THE VOTE, INC., GREGG PHILLIPS, and CATHERINE ENGELBRECHT,	§	
	§	
DEFENDANTS.	§	

PLAINTIFF'S MOTION FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION AND BRIEF IN SUPPORT

Plaintiff Konnech, Inc. ("Konnech") files this Motion for Temporary Restraining Order and Preliminary Injunction and Brief in Support and shows as follows:

PRELIMINARY STATEMENT

This is an action for temporary and preliminary injunctive relief arising out of Defendants True the Vote, Inc., Catherine Engelbrecht, and Gregg Phillips (collectively "Defendants") admitted hacking and theft of financial and other sensitive personal data of purportedly 1.8 million U.S. poll workers allegedly from a Konnech protected computer. As an initial matter, Konnech has never managed customer data for 1.8 million poll workers or even a small percentage of that many poll workers. But regardless, based on the extensive security measures Konnech has in place, Defendants could only access *any* of Konnech's data if they illegally hacked into and stole data from Konnech's protected computers. Defendants must be enjoined from taking any further unlawful action and to return the information they claim to have wrongfully stolen from Konnech.

First, Konnech will succeed on the merits of its claims because Defendants have repeatedly confessed their unlawful violation of the federal Computer Fraud and Abuse Act, 18 U.S.C.§ 1030,

et. seq., and the Texas Harmful Access by Computer statute. TEX. CIV. PRAC. & REM. CODE § 143.001; TEXAS PENAL CODE § 33.02. Specifically, Defendants claim that they and/or others working in concert with them gained unauthorized access to Konnech's protected computers and obtained personal information concerning U.S. poll workers. Indeed, Defendants admit they are under investigation by the FBI in connection with their unlawful conduct.

Second, Konnech will suffer immediate irreparable injury without injunctive relief because, based on Defendants' repeated confessions, they are interfering with Konnech's ability to control access to its protected computers and threatening to publicly disclose the data that they illegally obtained. Specifically, Defendants claim to have stolen data on 1.8 million U.S. poll workers—including personal identifying information, such as social security numbers, email addresses, phone numbers, and banking information—from what Defendants describe as an unsecured server and are threatening to publicly disclose it in advance of the 2022 midterm elections. As a result, Konnech will be immediately and irreparably harmed by a breach of security of Konnech's protected computers, disclosure of confidential information, the unauthorized use and/or disclosure of data from Konnech's protected computers, loss of confidence and trust of Konnech's customers, loss of goodwill, and loss of business reputation.

Third, the threatened injury to Konnech far outweighs any damages that an injunction might cause to Defendants. Defendants will not be damaged by enjoining them from committing further unlawful acts, by returning the information they stole from Konnech, or by describing how Defendants obtained data from Konnech's protected computers without authorization, so that there is no further unauthorized access to Konnech's protected computers in connection with the 2022 midterm elections.

And *fourth*, it is in the public's interest to enjoin conduct that the United States and Texas have found to be unlawful, to prevent the unlawful disclosure of personal identifying and banking information, and to benefit the public by increasing confidence in the U.S. election process.

Accordingly, Konnech is entitled to a temporary restraining order and preliminary injunction enjoining Defendants, directly or indirectly, and whether alone or in concert with others: (1) from accessing or attempting to access Konnech's protected computers; (2) to return to Konnech all property and data obtained from Konnech's protected computers, whether original, duplicated, computerized, handwritten, or any other form whatsoever; (3) from using, disclosing, or exploiting the property and data downloaded from Konnech's protected computers; (4) to preserve, and not to delete, destroy, conceal or otherwise alter, any files or other data obtained from Konnech's protected computers; (5) to identify each individual and/or organization involved in accessing Konnech's protected computers; (6) ordering Defendants to confidentially disclose to Konnech how, when, and by whom its servers were accessed without authority so that additional necessary security measures can be implemented by Konnech to maintain the integrity of the data therein in light of the upcoming midterm elections; and (7) ordering Defendants to identify all persons and/or entities, in Defendants' knowledge, who have had possession, custody or control of any information or data from Konnech's protected computers.

The Court should consider this Motion *ex parte*, because if Defendants or those acting in concert with Defendants learn about this action and the relief sought herein, Defendants or those acting in concert with Defendants may follow through on their threats to publicly release the data before the Court has an opportunity to consider this Motion, and may otherwise destroy evidence of their misconduct.

FACTUAL BACKGROUND[1]

In the summer of 2022, Defendants advertised an event they dubbed "The Pit," scheduled for August 13, 2022, at which they claimed they would disclose "devastating" information that, in their words, would be definitive proof that the 2020 Presidential Election was stolen from former President Donald Trump. The Pit was hosted by Defendants and attended by over 100 invite-only guests, handpicked by Defendants Engelbrecht and Phillips based on who they believed would be supportive of their conspiracy and who would best spread the disinformation they planned to disclose. After Defendants shut off the livestream of The Pit, Defendants disclosed that they had been secretly working on something they called "The Tiger Project," during which they allegedly discovered that Konnech had an unsecure server located in Wuhan, China, from which Defendants claim to have obtained U.S. election data.

One attendee of The Pit, who is actually the producer of Defendant Phillips' "Patriot Games" podcast, immediately posted a high-level summary of what was discussed by Defendants Phillips and Engelbrecht after the livestream ended. The post has been "ReTruthed" (the Truth Social equivalent of a Retweet) nearly 3,000 times, including by Defendant Phillips as an apparent confirmation of the event summary:

[1] A full recitation of the facts is contained in Plaintiff's Original Complaint.

(Ex. A-4.)

Specifically, Defendants claim that they, and/or others acting in concert with them, unlawfully used a password to access a Konnech server without authorization and downloaded the personal data on 1.8 million U.S. poll workers—including social security numbers, phone numbers, email addresses, and banking information. (*See* Exs. A-1, A-2, A-4.)

As an initial matter, Konnech has never managed customer data for 1.8 million U.S. poll workers or even a small percentage of that amount. But regardless, based on the extensive security measures Konnech has in place, Defendants could only access *any* of Konnech's data if they illegally hacked into and stole data from Konnech's protected computers.

To be clear, Konnech has never authorized Defendants, nor anyone acting in concert with them, to access Konnech's protected computers or to obtain, use, and/or disclose any data contained on those protected computers. (Ex. A, Yu Aff. at ¶ 5.) Konnech takes significant measures to protect the security and integrity of its protected computers, including controlling access to its offices, entering into confidentiality agreements with its customers and employees, and using two-factor authentication provided to a select group of Konnech employees with access to the protected computers which store poll worker data. (Ex. A, Yu Aff. at ¶ 3.)

Defendants also falsely and maliciously claim that the data they obtained by hacking into Konnech's protected computer demonstrates that Konnech is being used as a vehicle for the Chinese Communist Party to breach U.S. elections. (*See* Ex. A-2.) Defendants claim that they took the information they stole from Konnech to the FBI, but that the FBI subsequently opened an investigation of Defendants for gaining unauthorized access to Konnech's protected computers and stealing data from Konnech. (*See* Exs. A-1, A-3.)

Following The Pit, Defendants went on a media blitz to publicize their newly fabricated conspiracy theory in an unabashed effort to enrich themselves at the expense of Konnech. Defendant Phillips, in particular, appeared on several different podcasts and gave numerous interviews where he not only continued to spew baseless lies about Konnech, but he repeatedly confessed to hacking Konnech's servers and stealing its data.

For example, on August 23, 2022, Defendant Phillips appeared on the "Prophets and Patriots" video podcast where he described meeting his "guys" at a hotel room in Dallas, Texas, where they put "towels under the doors" like "some kind of a James Bond kind of thing," and proceeded to hack into a Konnech server. (*See* Ex. A-1.) Indeed, Defendant Phillips admitted on that podcast that they "took [Konnech's data] directly" and that Defendant True the Vote plans to publicly "release all of [Konnech's] data" through "drops" to subscribers to Defendants' website. (*Id.*) Defendant Phillips also admitted that Defendants are the subjects of an ongoing FBI investigation for their roles in allegedly hacking Konnech's server and stealing their data. (*Id.*)

Likewise, on an August 30, 2022 video podcast titled, "Here's How They'll Try to Steal the Midterms," Defendant Phillips again described how "[his] analysts" "brought [him] to Dallas into a hotel room at the Anatole Hilton Hotel" at "nearly midnight" where "they plugged one of their computers into the television" and began looking at Konnech's data on a server Defendants hacked into. (*See* Ex. A-2.) To be sure, Defendant Phillips admits that, on "that night, in mid-January of 2021, [he] personally witnessed the scrolling through millions and millions of records about Americans," which were obtained by gaining unauthorized access to Konnech's protected computer servers. (*Id.*) Defendant Phillips then further described how he "immediately drove down to Houston" and got Defendant Engelbrecht "to come over and meet [him]" that next

morning, where they came up with a plan to file a complaint with the FBI and turn over the data they allegedly stole. (*Id.*)

And on a September 2, 2022 video podcast hosted by Defendant Phillips called "Patriot Games,"—during which he admits the FBI accused him of being "the thief that stole the Chinese internet"—Defendant Engelbrecht confessed to how Defendants conspired to unlawfully access Konnech's protected computers, and how she and Defendant True the Vote "pulled in [Defendant Phillip's] team, and asked them to take a deeper dive" around the security of Konnech's software. (*See* Ex. A-3.)

Defendants are now threatening to publicly disclose, ahead of the 2022 midterm elections, all of the information they obtained by unlawfully accessing and downloading information from Konnech's protected computers (*see* Ex. A-1), for the purpose of damaging Konnech and discrediting the integrity of U.S. elections.

Defendants therefore admit to violating the federal Computer Fraud and Abuse Act and the Texas Harmful Access by Computer statute, and further admit to stealing information from Konnech that they intend to immediately disclose to the public. Unless restrained by the Court, Defendants will continue their illegal activities to the immediate and irreparable harm of Konnech.

ARGUMENT

A. Konnech Is Entitled to the Relief Sought

A plaintiff is entitled to a TRO and preliminary injunction where it shows: (a) the defendant's actions will cause irreparable harm to the plaintiff; (b) the relative lack of harm to the defendant if the TRO or injunction issues; (c) the public interest in issuing the TRO or injunction; and (d) the likelihood that the plaintiff will win on the merits of the lawsuit. *Lakedreams v. Taylor*, 932 F.2d 1103, 1107 (5th Cir. 1991) (affirming grant of preliminary injunction); *Florida Atlantic*

University Bd. of Trustees v. Parsont, 465 F. Supp. 3d 1279, 1288 (S.D. Fla. 2020) (issuing preliminary injunction in connection with violation of the CFAA); *MetroPCS v. Mohammed*, No. 3:16-cv-1946-L-BK, 2017 WL 2590108, at *7 (N.D. Tex., Apr. 24, 2017) (issuing permanent injunction in connection with violation of the CFAA).

The federal Computer Fraud and Abuse Act ("CFAA") prohibits unauthorized access to a "protected computer" for purposes of obtaining information, causing damage, or perpetrating fraud. *Quantab Techs. Ltd. v. Golevsky*, 719 F. Supp. 2d 766, 775 (S.D. Tex. 2010); 18 U.S.C. § 1030, *et. seq*. The CFAA is a criminal statute but also provides a private right of action for damages and injunctive relief when a violation of the CFAA, or a conspiracy to violate the CFAA, results in an aggregate loss of at least $5,000 to a plaintiff in a one-year period. 18 U.S.C. § 1030(c)(4). The term "loss" includes any investigative costs or expenses incurred by a plaintiff to assess, investigate, restore data, remediate, or respond to an offense. 18 U.S.C. § 1030(e)(11).

The CFAA defines a computer as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device[.]" 18 U.S.C. § 1030(e)(1). The term "protected computer" is further defined to include "a computer . . . which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B-C).

The CFAA thus has four elements: (1) a defendant intentionally accessed a protected computer; (2) without authorization or exceeding authorized access; (3) the defendant obtained

information; and (4) the plaintiff suffered damage or loss of at least $5,000. *See FAU Bd. of Trustees*, 465 F. Supp. 3d at 1289.

Similarly, under Texas Civil Practice and Remedies Code § 143.001, a "person who is injured or whose property has been injured as a result of a violation under Chapter 33, Penal Code, has a civil cause of action if the conduct constituting the violation was committed knowingly or intentionally." TEX. CIV. PRAC. & REM. CODE § 143.001. Texas Penal Code § 33.02 provides: "A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner." TEX. PENAL CODE. § 33.02(a). "Access" means to "approach, instruct, communicate with, store data in, retrieve or intercept data from, alter data or computer software in, or otherwise make use of any resource of a computer, computer network, computer program, or computer system." *Id*. The only apparent difference between the Texas Harmful Access by Computer statute and the CFAA is that, under the Texas statute, a defendant can be liable without obtaining information, and merely accessing a computer without effective consent is sufficient to establish liability.

Konnech provides election logistics software, called PollChief, that is used by governmental entities throughout the U.S. to recruit, train and schedule poll workers; coordinate the distribution of equipment and supplies to polling places; and dispatch support personnel to address technical and other issues. (Ex. A, Yu Aff. at ¶ 2.) It is therefore indisputable that Konnech's computers are used in or affect interstate commerce and, accordingly, Konnech's computers constitute a "protected computer" under the CFAA. (Ex. A, Yu Aff. at ¶¶ 2-3.)

Konnech's data is protected by various security measures, including two-factor authentication required for access. (Ex. A, Yu Aff. at ¶ 3.) Only a select group of Konnech employees that have been provided with that two-factor authentication have authority to access the

protected computers which contain poll worker data. (Ex. A, Yu Aff. at ¶ 3.) Konnech has never given consent to or authorized Defendants, nor anyone acting in concert with them, to access Konnech's protected computers or to obtain, use, and/or disclose any data contained on those protected computers. (Ex. A, Yu Aff. at ¶ 5.)

Defendants, however, admit to intentionally gaining, and conspiring to gain, unauthorized access to Konnech's protected computers, and obtaining information contained on Konnech's protected computers. (*See* Exs. A-1, A-2, A-3, A-4.) Specifically, Defendants, who did not have effective consent or authority to access any of Konnech's protected computers, claim that they gained unauthorized access to a server owned by Konnech using a "default password," and viewed and downloaded data pertaining to 1.8 million U.S. poll workers. (*Id.*); *Frisco Med. Ctr., L.L.P. v. Bledsoe*, 147 F. Supp. 3d 646, 659 (E.D. Tex. 2015) (granting summary judgment where evidence established defendants accessed, copied, and transferred plaintiff's files without authorization); *Muhammed v. State*, 331 S.W.3d 187, 193 (Tex. App.—Houston [14th Dist.] 2011, pet. ref'd.) (affirming jury verdict for hacking violation).

Konnech has suffered loss in an amount exceeding $5,000 in a one-year period, because it has been required to investigate and assess Defendants' claims, it has been required to conduct additional costly security audits, and it has expended other resources in responding to and assessing the need to remediate the offense. (Ex. A, Yu Aff. at ¶ 6.)

Accordingly, it is therefore substantially likely and, in fact, inevitable, that Konnech will win on the merits of its CFAA and Harmful Access by Computer claims given Defendants' repeated admission of their unlawful conduct. Konnech has thus shown a substantial likelihood of success on its CFAA and Harmful Access by Computer claims.

B. Konnech is Threatened with Immediate and Irreparable Harm

Unless the Court grants injunctive relief, Konnech will suffer immediate and irreparable harm by: (a) the unauthorized access to Konnech's protected computers; (b) the unauthorized use and/or disclosure of data from Konnech's protected computers; (c) interference with Konnech's control of its protected computers; (d) breach of security of Konnech's protected computers; (e) disclosure of confidential information contained on Konnech's protected computers; and (f) loss of confidence and trust of Konnech's customers, loss of goodwill, and loss of business reputation.

Courts have uniformly held that mere interference with an entity's control of its computer systems constitutes irreparable injury. *See FAU Bd. of Trustees*, 465 F. Supp. 3d at 1296 ("Unsurprisingly, federal courts around the country agree that the interference with an entity's control of its computer systems constitutes irreparable injury."); *Facebook, Inc. v. Power Ventures, Inc.*, 252 F. Supp. 3d 765, 782 (N.D. Cal. 2017), *aff'd*, 749 F. App'x 557 (9th Cir. 2019) ("[I]n accessing [the plaintiff's] computers without authorization, Defendants have interfered with [the plaintiff's] right to control access to its own computers and have acquired data to which Defendants have no lawful right in violation of the CFAA," thus causing irreparable injury); *Reliable Prop. Servs., LLC v. Capital Growth Partners, LLC*, 1 F. Supp. 3d 961, 965 (D. Minn. 2014) (finding "substantial threat of irreparable harm" based on the public dissemination of information after the defendant "unlawfully took volumes of detailed data" in violation of the CFAA); *Enargy Power Co. v. Xiaolong Wang*, No. 13-11348-DJC, 2013 WL 6234625, at *10 (D. Mass. Dec. 3, 2013) ("[P]revent[ing] Enargy from enjoying the uninterrupted use of its property . . . constitutes irreparable harm.").

If the Court were to permit Defendants to continue attacking and accessing Konnech's protected computers, Konnech could never be certain that it was adequately protecting its

customer's personal information, and its failure to protect that information could lead to questions about the integrity of the U.S. election process. (Ex. A, Yu Aff. at ¶ 7); *Mach 1, LLC v. Adaptisoft, LLC*, No. SA-21-CV-00114-XR, 2021 WL 6750834, at *2 (W.D. Tex. Feb. 16, 2021) (holding that enjoining defendant from damaging the system and requiring it to restore the system would prevent further irreparable harm). This, in turn will lead to loss of confidence and trust of Konnech's customers, and loss of Konnech's goodwill and business reputation. (Ex. A, Yu Aff. at ¶ 7); *see Mach 1*, 2021 WL 6750834 at *2 (finding irreparable injury in connection with CFAA violation where business "reputation will suffer as unreliable in an area where reliability is very important."); *Fletcher's Original State Fair Corny Dogs, LLC v. Fletcher-Warner Holdings LLC*, 434 F. Supp. 3d 473, 496 (E.D. Tex. 2020) ("Grounds for irreparable injury include loss of control of reputation, loss of trade, and loss of goodwill.").

And further, the unauthorized use and/or disclosure of data from Konnech's protected computers—which Defendants claim contains personal identifying information such as social security numbers, email addresses, phone numbers, and banking information of U.S. poll workers—would cause irreparable harm and would constitute a clearly unwarranted invasion of personal privacy. *See* TEX. BUS. & COMM. CODE § 521 (protecting personal identifying information); *see also U.S. Dept. of Defense v. Federal Labor Relations Authority*, 510 U.S. 487, 502 (1994) (holding that nondisclosure of "home addresses substantially outweighs the negligible FOIA-related public interest in disclosure" and "would constitute a 'clearly unwarranted invasion of personal privacy.'"); *Lamb v. Millennium Challenge Corp.*, 334 F. Supp. 3d 204, 214-15 (D. D.C. 2018) ("Generally, personal identifying information such as a person's . . . social security number may be protected under Exemption 6" of FOIA).

In the face of Defendants' admitted unauthorized access to Konnech's protected computers, and their further admission of their theft of data contained on said protected computers, Konnech seeks to prevent Defendants from further accessing Konnech's protected computers without authority, to return any data taken from Konnech's protected computers, and to not publicly disclose any such data or information wrongfully taken from Konnech's protected computers.

Konnech is plainly entitled to such relief under the law and cannot be adequately compensated through money damages. Therefore, an injunction should issue.

C. The Balance of the Hardships Weighs Decidedly in Konnech's Favor

When a defendant, such as Defendants here, engage in unlawful conduct prohibited by state or federal law, the Court need not consider hardship to the defendant. *See FAU Bd. of Trustees*, 465 F. Supp. 3d at 1297; *see also MediaOne of Delaware, Inc. v. E & A Beepers & Cellulars*, 43 F. Supp. 2d 1348, 1354 (S.D. Fla. 1998) (explaining that a defendant suffers no hardship when an injunction "will merely enjoin [the defendant] from conducting a business which is already prohibited by state and federal law"); *accord YourNetDating, Inc. v. Mitchell*, 88 F. Supp. 2d 870, 872 (N.D. Ill. 2000) (explaining the defendants "will suffer no legitimate harm of which they can complain if the [injunctive relief] is granted because they have no honest business hacking [the plaintiff's] system[.]").

If an injunction is not issued, Konnech will face significant harm to the security of its data, the theft of its secured and/or confidential information and systems, the privacy of its customers and, in turn, the integrity of U.S. elections. (Ex. A, Yu Aff. at ¶ 7.) On the other hand, an injunction would interfere only with the Defendants' unlawful access of Konnech's protected computers without any interruption to Defendants' legitimate business (if any). *See FAU Bd. of Trustees*, 465

F. Supp. 3d at 1297 ("Here, the balance weighs decidedly in FAU's favor. On the one hand, if an injunction does not issue, FAU will face 'significant harm to the security of its systems and data, theft of its secured, proprietary, and/or confidential information and systems, and privacy dangers to its students.'").

Accordingly, the balance of hardships weighs decidedly in favor of Konnech.

D. Injunction Is in the Public's Interest

Both the Texas Harmful Access by Computer statute and the CFAA are criminal statutes which provide for a private civil action, and, therefore, the public interest is advanced by enforcing compliance with the laws of Texas and the United States. *Id*. at 1298. In other words, "[s]ince the injunction does nothing more than prevent conduct that Congress has already deemed criminal, it necessarily advances the public interest." *Id*. Additionally, courts have routinely held that the "public has an interest in ensuring that computers are not accessed without authorization." *Facebook, Inc.*, 252 F. Supp. 3d at 785.

Moreover, the injunction implicates the privacy rights and interests of Konnech's customers and allegedly 1.8 million U.S. poll workers. *See FAU Bd. of Trustees,* 465 F. Supp. 3d at 1298 (finding injunction in the public's interest where defendant's unauthorized access of FAU's protected computer implicated the privacy rights of FAU students). In fact, it is paramount that the Court issue an injunction to secure the integrity of the upcoming 2022 midterm elections—and other future elections given that Defendants' misconduct will deter election logistic providers from providing their services, which are pivotal to running a smooth and trustworthy election process—which is undoubtedly in the public's interest.

An injunction issued against Defendants is therefore in the public's interest.

CONCLUSION

Konnech, Inc. respectfully requests that the Court grant this motion and issue a Temporary Restraining Order and Preliminary Injunction enjoining Defendants, directly or indirectly, and whether alone or in concert with others: (1) from accessing or attempting to access Konnech's protected computers; (2) to return to Konnech all property and data obtained from Konnech's protected computers, whether original, duplicated, computerized, handwritten, or any other form whatsoever; (3) from using, disclosing, or exploiting the property and data downloaded from Konnech's protected computers; (4) to preserve, and not to delete, destroy, conceal or otherwise alter, any files or other data obtained from Konnech's protected computers; (5) to identify each individual and/or organization involved in accessing Konnech's protected computers; (6) ordering Defendants to confidentially disclose to Konnech how, when, and by whom its servers were accessed without authority so that additional necessary security measures can be implemented by Konnech to maintain the integrity of the data therein in light of the upcoming midterm elections; and (7) ordering Defendants to identify all persons and/or entities, in Defendants' knowledge, who have had possession, custody or control of any information or data from Konnech's protected computers.

Dated: September 12, 2022

KASOWITZ BENSON TORRES LLP

By: */s/ Constantine Z. Pamphilis*
Constantine Z. Pamphilis
Attorney in Charge
Texas State Bar No. 00794419
SDTX Bar No. 19378
DPamphilis@kasowitz.com
Nathan W. Richardson
Texas State Bar No. 24094914
SDTX Bar No. 24094914

NRichardson@kasowitz.com
1415 Louisiana Street, Suite 2100
Houston, Texas 77002
(713) 220-8800
(713) 222-0843 (fax)

Attorneys for Plaintiff Konnech, Inc.

CERTIFICATE REQUESTING *EX PARTE* HEARING

I hereby certify that no notice has been given to Defendants or their counsel, and request that the Court consider this Motion *ex parte*, because if Defendants or those acting in concert with Defendants learn about this action and the relief sought herein, Defendants or those acting in concert with Defendants may follow through on their threats to publicly release the data before the Court has an opportunity to consider this Motion, and may otherwise destroy evidence of their misconduct.

/s/ Constantine Z. Pamphilis
Constantine Z. Pamphilis