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.)

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.