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 KONNECH, INC.'S REPLY IN SUPPORT OF ITS MOTION FOR PRELIMINARY INJUNCTION

Plaintiff Konnech, Inc. files this Reply in Support of its Motion for Preliminary Injunction ("Motion"), and shows the Court as follows:

PRELIMINARY STATEMENT

Defendants have presented no evidence whatsoever to oppose Defendants' Motion and made no effort to distinguish any of the cases that Konnech relies on. As such, since Konnech's evidence remains unchallenged, there is no genuine dispute of material fact, and the Court should grant this Motion on the papers.

First, it is undisputed that Konnech has a substantial likelihood of success on the merits of its claim that Defendants violated 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, in their Response, Defendants admit that they accessed Konnech's protected computer[1] by using a password to bypass its security. Under federal case law, the unauthorized use of any password constitutes hacking. In fact, what Defendants

[1] As used herein, the term "protected computer" shall have the same meaning as set forth in 18 U.S.C. § 1030.

claim to have done is no different than Defendants claiming that someone accidentally left the key in the lock to the front door to Konnech's offices, and that the Defendants then used that key to enter Konnech's offices without permission—it is still breaking and entering.

Aside from admitting liability for Konnech's hacking claims, Defendants incorrectly argue that Konnech has not pleaded a claim for hacking and that its claim should be dismissed because it was unable to find evidence of a breach of its systems. As established by the evidence attached to Konnech's Motion, Defendants have admitted to participating in the hacking of Konnech's computers and have admitted to possessing data taken from Konnech's computers without authorization. Simply because Konnech did not witness Defendants' unlawful intrusion into its computer system does not erase the fact that it occurred. Defendants had ample opportunity to submit sworn statements denying the veracity of their own statements but instead chose to rely on unsworn contradictory statements which do not constitute evidence.

The remainder of Defendants' Response is littered with political jargon that has no legal significance and is entirely irrelevant to the consideration of Konnech's Motion. Accordingly, Konnech respectfully requests that the Court grant its Motion for Preliminary Injunction.

ARGUMENT

I. There is a Substantial Likelihood that Konnech Will Succeed on the Merits

There is a substantial likelihood that Konnech will succeed on the merits of its federal and state hacking claims.

A. Defendants' Response admits to hacking

Defendants admit (Resp. at p. 8) to using a Konnech password to bypass a security feature of Konnech's protected computer without authorization which, according to federal case law, is an admission to violating the federal Computer Fraud and Abuse Act and the Texas Harmful

Access by Computer statute. Defendants have not presented any sworn denial of their prior admissions which have been established by Mr. Yu's[2] uncontroverted affidavit.

Specifically, Mr. Yu's affidavit establishes that Defendants have repeatedly and publicly stated at The Pit and on numerous podcasts that in January of 2021, Defendants, along with their "guys" and their "analysts" met at a Dallas, Texas hotel room 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 and take data on 1.8 million U.S poll workers. (*See* Mot., Ex. A-1, A-2.) Defendants even claimed 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* Mot. Exs. A-1, A-3.) Defendants have also stated that they have already given all of their "source material" to attendees at The Pit (*See* Mot. Ex. A-4)—which Konnech must assume means sensitive poll worker data, because that is what Defendants have claimed to have seen and taken from Konnech—and have otherwise stated their intent to "release all of [Konnech's] data" through "drops" to subscribers to Defendants' website. (*See* Mot. Ex. A-1.) Notably, Defendants have not submitted any evidence to deny these allegations, to correct their prior public admissions, or to otherwise refute Mr. Yu's affidavit.

Instead, Defendants contend that they cannot be liable for violations of the federal Computer Fraud and Abuse Act ("CFAA") or the Texas Harmful Access by Computer statute because they claim they used a default password to access a Konnech server in China. (Resp. at p. 8.) Defendants' attempted defense, however, is instead an admission of liability.

[2] Defendants try to claim that Mr. Yu's wrongful detention somehow proves their conspiracy theories in total disregard of Mr. Yu's presumption of innocence and despite the fact that the indictment is not even publicly available. Mr. Yu's arrest is entirely irrelevant to this civil action. But moreover, if anything, the LA County DA's statements concerning Mr. Yu's arrest underscores the importance of protecting the information Defendants claim to have stolen from Konnech. That is, information that Konnech had a right to possess; a right to possession never shared by Defendants.

In *Florida Atlantic University Bd. of Trustees v. Parsont*, the court issued a preliminary injunction based on the CFAA where the defendant, who was not a current student at the university, used passwords provided to him by current students to access the University's network. 465 F. Supp. 3d 1279, 1287 (S.D. Fla. 2020). In other words, the court found that, like here, even though Defendants claim that they merely used a password made available to them, the unauthorized use of that password which allowed access to a protected computer constituted a violation of the CFAA. *Id*.

Similarly, in *U.S. v. Nosal II*, a former employee used a current employee's password to access his former employers' protected computer. 844 F.3d 1024, 1038 (9th Cir. 2016). The court found that a showing that a party circumvents technological barriers is not necessary to prove that a party accessed a computer without authorization under the CFAA. *Id*. at 1032. Rather, all that is necessary is that a party used a password without authorization.

And in *HiQ Labs, Inc. v. LinkedIn Corp.*, a case which Defendants rely on in a futile effort to avoid liability (but which actually demonstrates that what Defendants admit to having done is unlawful), the Ninth Circuit was tasked with addressing the meaning of "without authorization" as used in the CFAA. 31 F.4th 1180, 1194-202 (9th Cir. 2022). There, the court determined that the term "without authorization" is "analogous to 'breaking and entering.'" *Id*. at 1197. The *hiQ* court thus distinguished between a public LinkedIn profiles, wherein one can access data contained thereon without any password, and a website which contains some sort of restriction or authorization requirement, such as a password. *Id*. ("[T]he prohibition on unauthorized access is properly understood to apply only to private information—information delineated as private through use of a permission requirement of some sort."). As such, "[w]ith regards to websites

made freely accessible on the Internet, the 'breaking and entering' analogue . . . has no application, and the concept of 'without authorization' is inapt." *Id*. at 1198.[3]

Unlike the data at issue in *hiQ*[4], the data Defendants claimed to have taken was indeed private and, in fact, it was admittedly restricted by a password which should have been a red flag to Defendants that the information was intended to be protected as private. (Resp. p. 8.) As Mr. Yu testified, Defendants had never been given authorization to use that password or to take that private data from a Konnech server. (*See* Mot. Exs. A at ¶ 5, A-1, A-2, A-3, A-4.) Using the "breaking and entering analogy" addressed by the *hiQ* court, what Defendants claimed to have done is no different than breaking and entering into Konnech's offices by using a key accidentally left in the front door.

Defendants have therefore admitted a violation of the CFAA and the Texas Harmful Access by Computer Statute. (Resp. at p. 8.)

B. The "Truth About Konnech" document does not exonerate Defendants for their admitted hacking

Defendants incorrectly rely on a "Truth About Konnech" document (which is not evidence) in a failed attempt to avoid liability for their admitted hacking.

Defendants make light of Konnech's "Truth About Konnech" document which resulted from Defendants' attack on Konnech and was intended to address its customers' concerns resulting therefrom. (Resp. at pp. 1, 5, 9-11.) In that document, Konnech specifically said that it found no

[3] Defendants also reference *Van Buren v. United States*, 141 S. Ct. 1648 (2021) in their Response. (Resp. at p. 9.) But *Van Buren* is entirely inapplicable. There, the Court merely held that there was no violation of the CFAA where an individual had authorization to access a protected computer, but had an improper motive for doing so. *Id*. at 1662. But here, Defendants have never been authorized or granted permission to access any non-public Konnech protected computer. (Mot. Ex. A at ¶ 5.)

[4] The court explained that "[t]he data hiQ seeks to access is not owned by LinkedIn and has not been demarcated by LinkedIn as private using such an authorization system." *Id*. at 1201.

breach of its system after conducting an internal investigation. But that doesn't mean it didn't happen, especially given Defendants' repeated public statements bragging about breaching a Konnech protected computer and taking Konnech's private data. (*See* Mot. Exs. A-1, A-2, A-3, A-4.)

Defendants' argument, in essence, is that simply because Konnech's internal investigation was unable to prove Defendants' misconduct, they are exonerated. To be clear, the "Truth About Konnech" document does *not* say that Konnech was not hacked, as Defendants characterize it. Rather, it merely says that Konnech was unable to find evidence of a breach on its system. Using the "breaking and entering" analogy again, Defendants would have this Court believe that it should be exonerated merely because a homeowner was unable to find evidence that their home was broken into, all while the criminal confesses to his unlawful activity.

Defendants' argument is simply baseless, and their own public admissions seal their fate.[5] (*See* Mot. Exs. A-1, A-2, A-3, A-4.)

C. Konnech pleaded a conspiracy between Defendants and other persons

As established above and in Konnech's Motion, there is a substantial likelihood of success that Konnech will prevail on its claims for violation of the CFAA and Texas Harmful Access by Computer Statute. *See FAU*, 465 F. Supp. 3d at 1291 ("[T]he CFAA does not limit its own reach to 'personal' or 'direct' access. To the contrary, it penalizes even *indirect* access to a 'protected computer.'"). But Konnech has also shown a substantial likelihood of success on its claims for

[5] Defendants further desperately try to avoid the consequences of their misconduct by claiming that this Court lacks jurisdiction because they claim Konnech has not "properly pled a federal claim." (Resp. 11.) To begin with, however, Defendants' Response is not a motion to dismiss Konnech's Original Complaint. But in any event, Defendants have pleaded a proper claim under the federal hacking statute, 18 U.S.C. § 1030, which is substantiated by Defendants' own admissions. And furthermore, Defendants' argument that Konnech has not alleged diversity jurisdiction because it has not alleged an amount in controversy exceeding $75,000 is belied by paragraph 16 of Konnech's Original Complaint, which specifically alleges that "the amount in controversy exceeds $75,000." (Doc. 1 at ¶ 16.)

conspiracy to violate the CFAA and Texas Harmful Access by Computer Statute. Konnech has pleaded a conspiracy between Defendants and other persons—not just between and amongst Defendants—based on their own statements of working with a "team" of "guys" and "analysts."

Defendants attempt to argue that the intracorporate conspiracy doctrine relieves them of liability because they incorrectly argue that Konnech has only pleaded a conspiracy between Defendants Engelbrecht, Phillips, and True the Vote. (Resp. at p. 7.) But Defendants ignore Konnech's allegations—based on Defendants' own statements—that they acted in concert with other persons. Indeed, Konnech's Original Complaint pleads how Defendant Phillips met "his guys" and his "analysts" at a Dallas hotel room where they proceeded to hack into a Konnech server. (*See e.g.*, Doc. 1 at ¶¶ 40, 41). And Defendants' counsel has represented to Konnech's counsel that this/these person/persons was "an independent contractor" (Doc. 16, Ex. D), or otherwise a "third party" not affiliated with Defendants. (Doc. 16, Ex. E.) Importantly, at the October 6, 2022 hearing, Defendants disclosed the identity of the person that they conspired with to breach Konnech's protected computers.

Defendants' argument to avoid conspiratorial liability fails in the face of their own admissions.

II. Konnech Will Be Irreparably Harmed by Defendants' Continued Misconduct

Defendants' admitted misconduct has and will continue to irreparably harm Konnech if Defendants are not enjoined.

Specifically, if Defendants are not enjoined from their unlawful conduct, Konnech will be 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. (Mot. Ex. A at ¶ 7); *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."); *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."); *Mach 1, LLC v. Adaptisoft, LLC*, No. SA-21-CV-00114-XR, 2021 WL 6750834, at *2 (W.D. Tex. Feb. 16, 2021); (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.").

Instead of putting forth admissible evidence to controvert Mr. Yu's affidavit testifying to irreparable harm, Defendants offer toothless lawyer argument (apparently) seeking to discredit Konnech's allegation that Defendants' misconduct caused Konnech to conduct additional costly security audits. (Resp. at p. 13.) To begin with, however, Konnech's security audits are entirely irrelevant to Konnech's allegations of irreparable harm. In fact, it is so off topic that it is unclear what Defendants are even trying to argue. In any event, that Konnech conducts regular security audits does not mean that it hasn't been forced to conduct *additional* audits. But again, the cost incurred for security audits is irrelevant to Konnech's claims of irreparable harm, which consists of the harm caused 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. (Mot. Ex. A at ¶ 7.)

Konnech will continue to be irreparably harmed if an injunction is not issued against Defendants.

III. Defendants Will Not be Harmed by a Preliminary Injunction Which Will Only Enjoin Unlawful Conduct, Which Is In the Public's Interest

A preliminary injunction will not enjoin any lawful conduct and, therefore the injunction cannot harm Defendants whatsoever. Instead, it will only enjoin unlawful conduct which is in the public's interest.

Section VII of Defendants' Response includes no legal or factual argument, and is instead nothing more than political fodder made in an effort to validate their conspiracy theories. Nevertheless, to the extent they attempt to argue, as the title of the section states, that "Konnech is seeking to have this Court enjoin investigation into election fraud," Defendants are mistaken.

To be clear, the preliminary injunction will not enjoin any lawful conduct. Rather, it will merely serve to prevent Defendants from engaging in *unlawful* conduct. Specifically, Konnech's proposed preliminary injunction defines "Konnech Data" to mean "any data on a Konnech Computer that is not intended to be available to the public or not otherwise in the public domain, including any U.S. poll worker data (including but not limited to their names, addresses, bank account numbers or social security numbers)." In other words, Defendants will only be enjoined from doing things that are prohibited by law.

As such, Defendants will not be harmed by the issuance of an injunction. *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[.]").

And "[s]ince the injunction does nothing more than prevent conduct that Congress has already deemed criminal, it necessarily advances the public interest." *FAU Bd. of Trustees*, 465 F. Supp. 3d at 1298; *see Facebook, Inc. v. Power Ventures, Inc.*, 252 F. Supp. 3d 765, 785 (N.D. Cal. 2017), *aff'd*, 749 F. App'x 557 (9th Cir. 2019) (explaining that the "public has an interest in ensuring that computers are not accessed without authorization.").

An injunction will only enjoin unlawful conduct and will not prevent any legally permissible investigation into purported election fraud.

CONCLUSION

Therefore, Konnech, Inc. respectfully requests that the Court grant its Motion for a Preliminary Injunction and issue the injunction against Defendants.

Dated: October 11, 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 OF SERVICE

I hereby certify that on October 11, 2022, true and correct copies of the above and foregoing were forwarded to all parties and counsel of record through the ECF filing system.

/s/ Nathan W. Richardson
Nathan W. Richardson