

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

KONNECH, INC.,

Plaintiff,

v.

TRUE THE VOTE, INC., *et al.*,

Defendants.

§
§
§
§
§
§
§
§

Civil Action No. 4:22-cv-03096

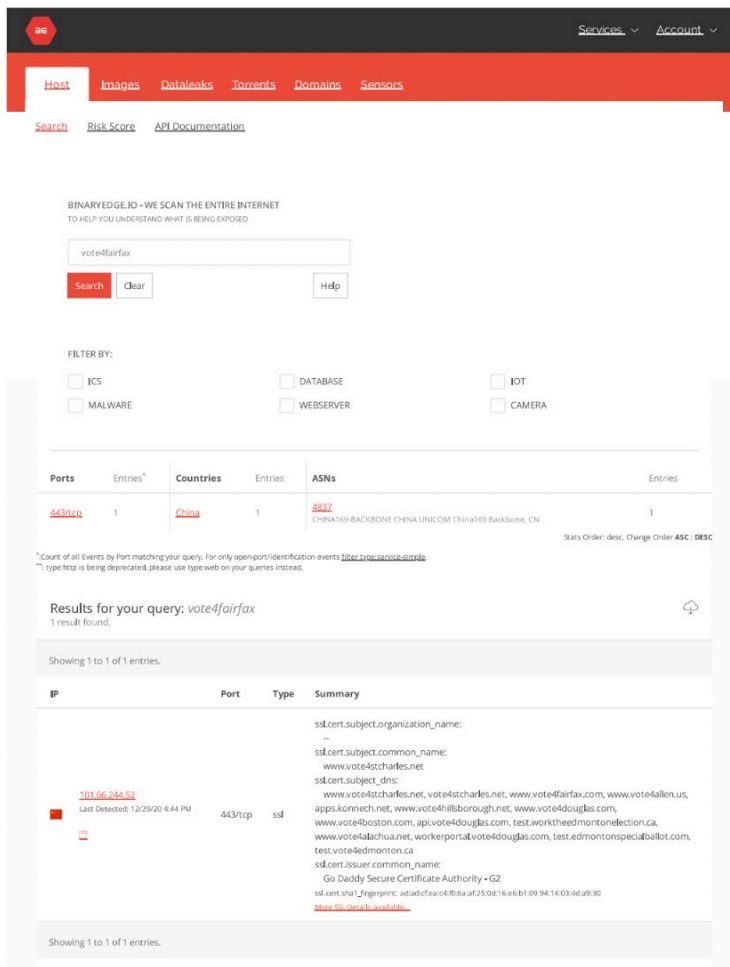
**DEFENDANTS’ OPPOSED EMERGENCY MOTION FOR LEAVE TO INSPECT
PROPERTY OF PLAINTIFF TO PREVENT FURTHER SPOILIATION OF EVIDENCE**

Defendants True the Vote, Catherine Engelbrecht, and Gregg Phillips (“Defendants”) move the Court for leave to inspect Plaintiff Konnech’s electronic storage devices, which are at this moment in the custody of Los Angeles County law enforcement. Working with Michigan law enforcement, Los Angeles County law enforcement seized the storage devices in the course of executing a lawful search warrant on Konnech’s headquarters in Michigan. Konnech’s president and CEO Eugene Yu has filed a motion to return property, which is pending before the 30th Department of the Los Angeles County Superior Court. The motion has been continued multiple times and is now set for consideration on March 2, 2023. The data stored on the devices is critical to the merits of this case and is or shortly will be the subject of several discovery requests. Defendants are seeking Court intervention before the devices are returned to Yu and Konnech in Los Angeles. Were that to happen before a copy is made, there is an unacceptable risk of spoliation. Supporting this motion, Defendants state as follows:

I. Konnech Has Made a Practice of Concealing Compromising Information from Its Customers and Regulatory Agencies.

Early in 2021, Defendant Gregg Phillips learned Konnech was hosting on Chinese servers the election-related domain names of its U.S.-based customers (including Vote4Fairfax.com,

Vote4Boston.com, Vote4Hillsborough.net), as well as what appear to be Chinese election system websites (e.g., 2dmeeting.com and 2dmeeting.cn), and the URL for the Konnech app (app.konnech.com) its American customers use. This means any customer data transmitted by means of Konnech’s customer-facing apps necessarily goes through an insecure server in China. Shown immediately below is a Binary Edge screenshot dated 12/29/20 listing Konnech-managed domain names hosted on a server in China sitting on Unicom, the Chinese Internet “backbone”:



The individual who reportedly obtained access to the data stored on the Chinese server, had been able to get ahold of it using the *default password* that came from the manufacturer. See Compl., ¶42; Tr. Gregg Phillips, October 27, 2022, Hearing at 94-95 (Ex. A). Once Defendants

made this information public, as was their right, Konnech sued them for defamation and bizarrely for unauthorized computer access, sought an injunction to try to silence them, and then moved the same data to another server, but this time one located in the United States. *See* Ex. B (Binary Edge screenshot dated 11/1/22).

Defendants have advised the public that Konnech was not only storing personal identifying information of American election workers and American customer data on insecure servers in China, but that it was permitting unvetted nationals based in China access to the China-based servers and to the software itself. Former Konnech employee Grant Bradley’s complaint, filed in Michigan state court on December 22, 2022 (*see* Ex. C, Verified Complaint and Jury Demand of Grant Bradley), echoes these concerns. Mr. Bradley alleges in his complaint as follows:

- In violation of its contracts with U.S.-based customers, Konnech provided programmers in China “private data of [U.S.-based] election workers, to include social security numbers and other identifying information.” Mr. Bradley “witnessed customer’s [sic] data (specifically poll watcher [sic] information) being made accessible to foreign nationals in China.” Compl. ¶3;
- Konnech’s election logistics software was (and may still be) substantially developed by “developers, designers and coders” who are “all Chinese nationals based out of Wuhan, China.” Compl. ¶15;
- Konnech initially identified these Chinese nationals as employees, but “in response to political pressure to sever ties with China,” Konnech, having “no intention of severing the relationship with the Chinese nationals . . . hired them back as independent contractors and assigned to them the exact same responsibilities they held as employees.” Compl. ¶16.

Los Angeles County was a Konnech customer. On October 4, 2022, the Los Angeles County District Attorney's Office, working with local law enforcement, seized all Konnech's computer servers from its corporate headquarters in Michigan, as well as all computers, cell phones and external electronic storage devices in the possession of Konnech's CEO, Eugene Yu. The seizure in Michigan pursuant to a lawful search warrant for the headquarters was executed more or less simultaneously with the issuance of a criminal complaint against Mr. Yu. Forensic cybersecurity firm Cain & Associates was tasked with assisting the DA's Bureau of Investigation in executing the search warrant on Konnech's headquarters.

Harry Haury, CEO of Cain & Associates, in summary stated that Konnech's data security system "amounted to by far the worst example of complete disregard or negligence regarding the protection of PII and sensitive data I have ever seen. We discovered a data breach of U.S. data, which is classified as a 'total loss of control'." *See* Ex. D, Affidavit of Harry Haury, ¶4. Mr. Haury states, in Paragraph 5 of his Affidavit, that Cain & Associates found volumes of evidence, on the seized devices, relevant to this case, and that Cain:

- confirmed multiple instances of Konnech hosting, on servers based in China, U.S. citizens' personally identifiable information (PII);
- found evidence in private company messages that software code was being developed, tested, and maintained in China;
- confirmed that Konnech was providing administrative credentials to Chinese developers;
- has evidence that Konnech employees have shared election-related data through, from, and on Chinese servers and applications;

- has evidence in metadata pulled from relevant files indicating Eugene Yu was involved in developing Chinese government (i.e., Wucheng District People’s Congress) election software; and
- has evidence showing Konnech is associated with several companies based in mainland China that appear to be associated with if not subsidized by the Chinese government.

Curiously, from the time Konnech filed its Complaint six months ago, when it claimed Defendants had violated the Computer Fraud and Abuse Act (CFAA), through the present – including an amendment and several well-researched motions and responses, Konnech has never claimed ownership of the server in China – the contents of which Defendant Gregg Phillips witnessed. Instead, Konnech’s strategy has been to quote Defendants’ comments about the server but either to remove any reference to China *or* to insert that Defendants “falsely” claim the server was in China.¹ In fact, Plaintiff has *disclaimed* ownership of the only allegedly “accessed” server in question, the one in China. In Paragraphs 2, 25, and 50 of its Complaint, Konnech repeats verbatim the mantra “All of Konnech’s U.S. customer data is *secured and stored exclusively on protected computers located within the United States.*”² (Emphasis added.)

Why would Konnech so openly expose half its case immediately to dismissal for failure to state a claim under the CFAA by failing either (1) to identify a particular computer that was

¹ See Compl. ¶¶24 (alleging “Defendants *falsely* claimed that they discovered that Konnech had an unsecured server located in Wuhan, China”), 40 (“Defendants have also *falsely* accused Konnech of maintaining unsecure Chinese servers”), 46 (“Defendants have *falsely* accused Konnech of storing sensitive and personal data . . . on servers in China, and otherwise running their election logistics application through Chinese servers”), 47 (“Defendant Phillips *falsely* claimed that Konnech ‘left a database open that had the personal identifying information of over a million Americans living on an open server in China’”), 48 (“Defendant Phillips *falsely* claimed that Konnech’s election software ‘apps were running from China, the database is running in China’”) (emphases added).

² Notwithstanding this dispute and Konnech’s refusal or inability to identify whatever server was supposedly “accessed”, the Court granted Konnech’s *ex parte* requests for a TRO and preliminary injunction to force Defendants to take certain actions with respect to an unidentified “Konnech protected computer” that Defendants had said was in China and that Plaintiff insisted (without identifying it) must have been in the United States.

allegedly accessed or (2) to claim ownership of the China-based server it claims Gregg Phillips “*admitted*” to accessing? Because the presence of that server in China is acutely embarrassing to Konnech, for it means that either Konnech:

1. got hacked by a hacker who moved Konnech’s data to a server in China, which was later accessed by the person who showed the data to Defendant Phillips, or
2. knowingly kept American election worker data, customer domain names, and the apps through which its customers’ data passed on a server in China, where it was accessible to and potentially manipulated by unvetted Chinese nationals residing in China.

If Konnech’s data were hacked and moved onto insecure servers in China, then its customers would be infuriated. But if Konnech’s customers’ data was illegally, or in breach of customer contracts, knowingly stored on a computer in China, and worked on by Chinese nationals based there, then the customers would be even more upset, and would likely cancel their contracts with Konnech or even bring legal action against Konnech – as Los Angeles County did.

Defendants have brought this motion precisely because where someone has a lot to hide, that someone will do whatever it takes to hide it.

II. Since Konnech Filed the Instant Lawsuit, It Has Attempted to Conceal or Destroy Evidence and Tamper with Witnesses.

Following the seizure of Konnech’s devices by Los Angeles County, its forensic investigators worked with one or more confidential informants within Konnech to get access to various Internet-connected accounts used by Konnech, such as Jira (used by programmers to report bugs and add software development tasks, or tickets), Konnech’s internal email system, and the China-based collaboration service DingTalk. However, by about the fourth day following the seizure, and about one month *after* Plaintiff had filed its Complaint against Defendants, someone with administrative access to these accounts, containing evidence relevant to this case, began

systematically shutting off access to the data in them, one by one. *See* Aff. Harry Haury, ¶7. The evidence that was in those accounts, having been successfully hidden, has never been recovered.

But Konnech was only just beginning to try to cover its tracks. According to the then-General Manager of Konnech Australia, about a month later, in November 2022, Konnech instructed him to erase and move data potentially relevant to this case. *See* Ex. E (Affidavit of Brian Glicklich).

Similarly, Grant Bradley, the now-former Konnech employee, was instructed by his Konnech supervisors (a) not to cooperate with law enforcement during and after the execution of the search warrant on Konnech's headquarters, and (b) to mislead Konnech's customers concerning the use of U.S. election worker data by Chinese nationals based in China. (Compl.). Mr. Bradley states he was "told by his superiors to say outwardly to customers that election worker data was not stored overseas, not available to foreign nationals, and that they had no idea why Defendant Yu was arrested." Compl. ¶2. Mr. Bradley's supervisors at Konnech also gaslighted him about their use of China-based programmers by telling him, falsely, that "everyone [other software companies like Microsoft and Apple] was doing it." Compl. ¶20.

Mr. Bradley claims Konnech supervisors told him to lie to any customers who asked whether U.S. election worker data was being stored overseas, whether the data was readily available to Chinese or other foreign nationals, or whether other companies also employed Chinese nationals to handle sensitive information. Compl. ¶2. Mr. Bradley was also told "by his supervisors not to speak with the police or cooperate in their investigation of Defendants Yu and Konnech's activities." Compl. ¶25.

III. Konnech Has Intimidated Persons Cooperating with Law Enforcement.

Mr. Bradley's Complaint details numerous other efforts by Konnech to interfere with the administration of justice. Mr. Bradley spoke "to his direct supervisors about his concern that these foreign nationals had access to the data," Compl. ¶20, and told his supervisors, "he would not tell customers that their data is not stored overseas or not accessible by the Chinese programmers." *Id.* ¶27. Mr. Bradley alleges Konnech terminated him in retaliation for his cooperation with the Los Angeles County District Attorney's Office and for refusing to lie to customers about Konnech's employment of Chinese nationals based in China in connection with the use of software relating to U.S. elections and polling. *Id.* ¶1. In fact, Konnech CEO Eugene Yu terminated Mr. Bradley within one hour of Mr. Bradley telling one of his supervisors that he would not lie to customers. *Id.* ¶30.

ARGUMENT

The relief sought here is routinely granted in analogous situations where the moving party must seek court intervention to preserve evidence for civil discovery in the interest of justice. *See Matter of Vuitton et Fils S.A.*, 606 F.2d 1, 3 (2d Cir. 1979) (granting TRO, *ex parte*, to prevent destruction of trademark-infringing defendants' inventory of counterfeit Vuitton merchandise); *Intel Corp. v. Rivers*, No. 2:18-CV-03061-MCE-AC, 2019 WL 4318583, at *1 (E.D. Cal. Sept. 12, 2019) (noting party "stipulated to entry of a Temporary Restraining Order which allowed inspection of his home computer by a third-party investigator" following evidence the party had previously destroyed evidence on a thumb-drive); *Thomas v. Trustees of Indiana Univ.*, No. 118CV03305TWPDM, 2018 WL 6074505, at *7 (S.D. Ind. Nov. 21, 2018) (temporarily restraining party "from allowing spoliation of evidence of" mold during the remediation of that mold); *Landus Coop. v. New Coop., Inc.*, No. 21-CV-3003-CJW-MAR, 2021 WL 1095333, at *2

(N.D. Iowa Feb. 3, 2021) (granting TRO where the “record suggests that there may have been an attempt to destroy evidence”); *Verizon California Inc. v. Lead Networks Domains Priv. Ltd.*, No. CV 09-613-ABC (CWX), 2009 WL 10700112, at *11 (C.D. Cal. Feb. 17, 2009) (granting TRO because “[w]hile under normal circumstances commencing litigation would itself be sufficient to put a defendant on notice that all materials potentially usable as evidence should be preserved,” where the non-moving party had “taken . . . many affirmative steps to conceal” evidence, “these are not normal circumstances”).

The evidence Defendants seek to preserve is not only relevant but may be outcome-determinative if this case proceeds on the merits. In the months after Konnech filed its Complaint, it actively sought to destroy evidence of its activities and to persuade employees to lie about (and to fire them when they would not) the very activities at the heart of Plaintiff’s defamation and computer access claims. Under the Federal Rules of Civil Procedure, Rule 26(b)(1),

[p]arties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party ... For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.

Although such discovery need not be proven to be admissible at trial, it is discoverable if, as here, it is “reasonably calculated to lead to the discovery of admissible evidence.” FED. R. CIV. P. 26. Courts will order even *direct* access to a responding party's electronic storage devices (which is not requested here) when there is, as here, some direct relationship between the electronic storage device and the plaintiff’s claim itself. *See In re Weekley Homes, L.P.*, 295 S.W.3d 309, 317 (Tex. 2009) (citing *Cenveo Corp. v. Slater*, No. 06–CV–2632, 2007 WL 442387, at *2, 2007 U.S. Dist. LEXIS 8281, at *4 (E.D.Penn. Feb. 2, 2007); *Frees, Inc. v. McMillian*, Civil Action No. 05–1979, 2007 WL 184889, at *3, 2007 U.S. Dist. LEXIS 4343, *9 (W.D.La. Jan. 22, 2007));

Ameriwood Indus., Inc. v. Liberman, No. 4:06CV524–DJS, 2006 WL 3825291, at *1, 2006 U.S. Dist. LEXIS 93380, at *5 (E.D.Mo. Dec. 27, 2006); *Balboa Threadworks, Inc. v. Stucky*, Case No. 05–1157–JTM–DWB, 2006 WL 763668, at *4, 2006 U.S. Dist. LEXIS 29265, *12 (D.Kan. Mar.24, 2006).

In *Ameriwood Industries*, Ameriwood sued several former employees claiming they improperly used Ameriwood's computers, confidential files, and confidential information to sabotage Ameriwood's business by forwarding customer information and other trade secrets from Ameriwood's computers to the employees' personal email accounts. 2006 WL 3825291, at *1, *3, 2006 U.S. Dist. LEXIS 93380, at *2, *9. Based in part on the close relationship between Ameriwood's claims and the employees' computer equipment, the trial court approved “allowing an expert to obtain and search a mirror image of [the employee] defendants” hard drives. *Id.*, 2006 WL 3825291, at *1, 2006 U.S. Dist. LEXIS 93380, at *6.

Similarly, in *Cenveo Corp.*, a company sued several former employees for improperly using its computers, confidential trade information, and trade secrets to divert business from Cenveo to themselves. 2007 WL 442387, at *1, 2007 U.S. Dist. LEXIS 8281, at *1. Borrowing from *Ameriwood*, the district court issued a similar order “[b]ecause of the close relationship between plaintiff's claims and defendants' computer equipment.” *Id.*, 2007 WL 442387, at *2, 2007 U.S. Dist. LEXIS 8281, at *4. Finally, in *Frees*, a former employee was sued for using company computers to remove certain proprietary information. 2007 WL 184889, at *1, 2007 U.S. Dist. LEXIS 4343, at *2. Noting that the employee's computers would be “among the most likely places [the employee] would have downloaded or stored the data allegedly missing,” *id.*, 2007 WL 184889, at *2, 2007 U.S. Dist. LEXIS 4343, at *5, the court ordered direct access be granted to the employee's work and home computers. *Id.* The court in *Weekley Homes* focused on the nature

and extent of the “direct relationship between the electronic storage device and the claim itself.” *Id.* at 317–19.

Here, it is Plaintiff that has brought claims that directly implicate its computer devices, their locations, the data on them, and the identity of those who worked on them. Indeed, Plaintiff alleged that Defendants violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g), by accessing Plaintiff’s computer devices, making those devices clearly and directly relevant to its claims. Plaintiff also sued for defamation related to Defendants’ statements regarding Konnech’s Chinese connections, including the existence of devices in China, the storage of data there, and the work by Chinese nationals based there. The contents of Plaintiff’s computer devices are thus unquestionably relevant to this case, including:

- Evidence of any access of those computers by third parties, including Defendants.
- Evidence that Plaintiff employed persons located in China, and used computer servers located in China.
- Evidence that Plaintiff terminated Chinese nationals as employees, in response to negative publicity, and quietly rehired them as contractors.
- Evidence that Plaintiff gave every user super-user access to sensitive data and software code.
- Evidence that Plaintiff attempted to influence witnesses and remove evidence.
- Evidence supporting the other claims Defendants have made in this matter, as corroborated by LA County and Grant Bradley.

Here, discovery has only just begun, with Defendants having served the first discovery in the case on February 23, 2023, pursuant to the Joint Discovery and Case Management plan filed a day earlier. Plaintiff’s counsel have explained that they cannot participate in most discovery until the devices seized by LA County are returned. However, the conduct of Konnech itself has created an exigent circumstance that militates against returning Konnech’s devices to it directly, for further spoliation of evidence.

Defendants are concerned about these reports of Konnech’s coercion, witness tampering, evident intent to spoil evidence and to violate the law, and plain obstruction. Such behavior is an affront to the fair administration of justice. In an abundance of caution, it is therefore appropriate that before the seized devices are returned to Plaintiff, the Court should impose a brief pause and ensure that an independent, expert third party can take a mirror-image³ of them. *See Wynmoor Cmty. Council, Inc. v. QBE Ins. Corp.*, 280 F.R.D. 681, 686 (S.D. Fla. 2012) (granting motion to inspect “in light of the evidence of an unusually large spate of document shredding”). Ordering a forensic examination to be performed by an independent third-party forensic analyst is particularly appropriate where, as here, it is not reasonably possible for the trial court to describe, in advance, search protocols with sufficient precision to capture only relevant, non-privileged information. *In re Clark*, 345 S.W.3d 209, 213 (Tex.App.—Beaumont 2011, orig. proceeding).

Accordingly, with respect to the seized devices, including but not limited to those listed in Exhibit F, Defendants request the following⁴:

1. Within five (5) days from the date of the Court’s order, the parties shall jointly select a qualified independent third-party forensic examiner to conduct an examination of seized

³ “A forensic image, otherwise known as a ‘mirror image’ will replicate bit for bit sector for sector, all allocated and unallocated space, including slack space, on a computer hard drive. A mirror image contains all the information in the computer, including embedded, residual, and deleted data.” *Wynmoor Cmty. Council, Inc. v. QBE Ins. Corp.*, 280 F.R.D. 681, 686–87 (S.D. Fla. 2012) (citing cases; cleaned up). “Forensic imaging preserves everything on the device at the time the image was made and makes the information accessible for later review.” *See BridgeTower Opco LLC v. Workforce Rsch. Grp. LLC*, No. 4:21-CV-02999, 2023 WL 361779, at *2 (S.D. Tex. Jan. 23, 2023). “Forensic imaging of computer storage devices and data sources is specifically designed to protect the integrity of the digital evidence and to allow recovery of all data that can potentially include hidden, erased, or encrypted files.” *Id.* (citation omitted; cleaned up). “Forensic imaging is the preferred method of data preservation.... A forensic image preserves the evidence and maintains the complete original storage media in its entirety.” *Id.*

⁴ For examples of how courts carefully structure such orders, *see In re Honza*, 242 S.W.3d 578, 583 (Tex. App. 2008) (citing *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 653-54 (D. Minn. 2002); *Rowe Ent., Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421, 433 (S.D.N.Y. 2002); *Simon Prop. Grp. L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 641-42 (S.D. Ind. 2000); *Playboy Enterprises, Inc. v. Welles*, 60 F. Supp. 2d 1050, 1055 (S.D. Cal. 1999)); *see also Benzion v. Vivint, Inc.*, No. 12-61826-CIV, 2013 WL 12304563, at *4 (S.D. Fla. Sept. 20, 2013).

devices. If the parties cannot agree on a forensic examiner, each party shall submit its recommendations to the Court, and the Court will select the expert.

2. Immediately upon being selected, the independent expert and anyone working with him or her shall sign a confidentiality agreement as required by any Protective Order entered in this case and the expert shall serve as an officer of the Court such that to the extent such expert has direct or indirect access to information protected by attorney-client privilege, such disclosure will not result in any waiver of privilege.
3. The examination of the devices shall be limited to data from the period between January 1, 2020, and October 4, 2022, including examining whether any responsive documents or data have been transferred or deleted from any hard drive or other storage device.
4. The independent expert shall image the hard drives and other storage devices of all seized equipment. The expert shall be allowed to hire other outside support if necessary in order to mirror-image the seized devices. Any outside support shall be required to sign the same confidentiality order.
5. The cyber recovery from the devices should be conducted by one or more qualified teams using FBI/DOJ standard recovery techniques either bonded or under affiant pledges. *See* Aff. Harry Haury at ¶9.
6. The experts shall attempt direct recovery from the original devices, and if that should prove to be impracticable, they shall use bit-by-bit full-disk images. To maintain a record of chain of custody, digital hashes shall be used. *Id.*, ¶10.
7. The independent expert shall provide the results to the Court and Plaintiff's counsel prior to production to defense counsel, and Plaintiff shall have thirty (30) days from receipt of

the results to file a motion for protective order regarding objectionable matter disclosed in the results.

8. Defendants shall respond to Plaintiff's objections, and those objections will promptly be adjudicated by the Court. The expert shall securely retain the copies of the data pending adjudication and until otherwise ordered by the Court.
9. If Plaintiff does not object within thirty (30) days of receipt of the expert's results, the findings shall be provided to Defendants.
10. Contemporaneous with the report on his or her results, the expert shall provide to Plaintiff and the Court a signed affidavit detailing the steps he or she took to examine Plaintiff's devices.
11. Because Plaintiff benefits from its counsel getting a mirror-image of its devices while Plaintiff expeditiously gets its devices back, costs shall be borne equally by Defendants and Plaintiff, unless the examiner (or Defendants) finds relevant documents that Plaintiff or someone on its behalf transferred or deleted.

In the alternative, a federal court may "issue preservation orders as part of its inherent authority to manage its own proceedings." *Gambino v. Hershberger*, No. CV TDC-16-3806, 2017 WL 2493443, at *3 (D. Md. June 8, 2017), *aff'd*, 700 F. App'x 272 (4th Cir. 2017); *see also Kemper Mortg., Inc. v. Russell*, No. 3:06-CV-042, 2006 WL 4968120, at *7 (S.D. Ohio May 4, 2006) (enjoining party from "[d]estroying or deleting, directly or indirectly, any documents or electronically stored information, including any information stored on computers" that contain relevant information). If the Court does not grant a TRO putting the seized devices into the care of an independent party, Defendants would ask that the Court issue a preservation order to Konnech. But Defendants maintain that Konnech already knew it should preserve evidence last

fall, when it filed its Complaint, while shortly thereafter the evidence indicates a risk that Konnech endeavored to destroy evidence, cause others to lie about evidence, and shut down investigators' access to it. Thus, the safest course here is to have an independent expert mirror the seized devices before returning them to Konnech.

Respectfully Submitted,

GREGOR | WYNNE | ARNEY, PLLC

By: /s/ Michael J. Wynne
Michael J. Wynne

Texas State Bar No. 0078529
SDTX No. 0018569
Cameron Powell
DC Bar No. 459020
909 Fannin Street, Suite 3800
Houston, Texas 77010
Telephone: (281) 450-7403
mwynne@gwafirm.com
cpowell@gwafirm.com

**ATTORNEYS FOR DEFENDANTS TRUE THE
VOTE, INC., CATHERINE ENGELBRECHT,
AND GREGG PHILLIPS**

CERTIFICATE OF CONFERENCE

I hereby certify that I have communicated with lead counsel for Plaintiff and that as of this filing, we have not yet received a response with regard to this particular motion. We have every reason to expect based on prior communications that Plaintiff is opposed to this motion and will amend this certificate immediately if that turns out not to be the case.

By: /s/ Michael J. Wynne
Michael J. Wynne

CERTIFICATE OF SERVICE

I hereby certify that on this 24th day of February 2023, this document was electronically filed with the Clerk of Court using the CM/ECF system which will automatically send email notifications of the filing to all attorneys of record.

By: /s/ Michael J. Wynne
Michael J. Wynne

EXHIBIT A

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS

THE HONORABLE KENNETH M. HOYT, JUDGE PRESIDING

KONNECH, INC.,)	Cause No. 4:22-cv-03096
)	
Plaintiff,)	
)	
vs.)	
)	
TRUE THE VOTE, et al.,)	
)	
Defendants.)	
)	

HEARING

OFFICIAL COURT REPORTER'S TRANSCRIPT

Houston, Texas

October 27, 2022

APPEARANCES:

On behalf of the Plaintiff:
 Constantine Z. Pamphilis, Esq.
 Nathan Richardson, Esq.

On behalf of the Defendants:
 Brock Cordt Akers, Esq. (Not present)
 Michael John Wynne, Esq
 John C. Kiyonaga, Esq.

Reported By: Nichole Forrest, CSR, RDR, CRR, CRC
 Certified Realtime Reporter
 United States District Court
 Southern District of Texas

Proceedings recorded by mechanical stenography.
 Transcript produced by Reporter on computer.

EXAMINATION INDEX

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

WITNESSES

PAGE

GREGG PHILLIPS

Direct Examination By Mr. Wynne 29
Cross-Examination By Mr. Pamphilis 37

CATHERINE ENGELBRECHT

Direct Examination By Mr. Wynne 106
Cross-Examination By Mr. Richardson 109
Redirect Examination By Mr. Wynne 166

1 around and trying to find things. But we also do
2 geospatial research.

3 THE COURT: Were you planning to put the
4 names of the individuals who worked for the Harris
5 County polling, Bexar County polling, all of that data
6 that you said that you saw, were you planning to post
7 that data on a public venue?

8 THE WITNESS: No, sir.

9 THE COURT: Does this sound familiar to
10 you: Gregg and Catherine, GC -- that's you, Gregg and
11 Catherine -- stumbled onto voting software used to
12 corroborate elections. Was left with default
13 password.

14 What is a default password?

15 THE WITNESS: A password that the software
16 would be shipped with.

17 THE COURT: Is what?

18 THE WITNESS: When they ship it to be
19 installed.

20 THE COURT: That means that someone has
21 intercepted a password?

22 THE WITNESS: No, sir. It ships with the
23 password. I think that is what it's referring to.

24 THE COURT: No. I'm asking you what
25 you're referring to.

1 It says here: You were left with -- you
2 used to coordinate the elections, was left with
3 default password of database.

4 What are you talking about?

5 THE WITNESS: Like I said, a password that
6 would be shipped with the software.

7 THE COURT: And so the software you're
8 referring to is what?

9 THE WITNESS: I don't recall. I mean,
10 do --

11 THE COURT: We're talking about this
12 software. We're talking about this data.

13 THE WITNESS: Well, I don't know that we
14 are or aren't. We could be talking about the
15 Open.INK.

16 THE COURT: But you're the one talking
17 about it.

18 THE WITNESS: Right. But I don't know if
19 that's what I was referring to.

20 THE COURT: Well, you said you stumbled
21 onto voting software used to coordinate elections.

22 That is what Konnech does, isn't it?

23 THE WITNESS: I think it's one of the
24 things they do.

25 THE COURT: Well, do they do it or not?

EXHIBIT B

[Host](#) [Images](#) [Dataleaks](#) [Torrents](#) [Domains](#) [Sensors](#)

[Search](#) [Risk Score](#) [API Documentation](#)

BINARYEDGE.IO - WE SCAN THE ENTIRE INTERNET

TO HELP YOU UNDERSTAND WHAT IS BEING EXPOSED

Search... Example: country:FR port:443

FILTER BY:

- ICS
- DATABASE
- IOT
- MALWARE
- WEBSERVER
- CAMERA

Ports	Entries*	Countries	Entries	ASNs	Entries
443/tcp	3	United States	3	14103 ACDNET-ASN1, US	2
				8075 MICROSOFT-CORP-MSN-AS-BLOCK, US	1

Stats Order: desc. Change Order **ASC** : **DESC**

*: Count of all Events by Port matching your query. For only open-port/identification events [filter type:service-simple](#).
 **: type:http is being deprecated, please use type:web on your queries instead.

Results for your query: *vote4fairfax.com*
 3 results found.

Showing 1 to 3 of 3 entries.

IP	Port	Type	Summary
75.75.210.242 Last Detected: 11/1/22 6:33 AM	443/tcp	ssl	ssl.cert.subject.organization_name: -- ssl.cert.subject.common_name: www.vote4stcharles.net ssl.cert.subject_dns: www.vote4stcharles.net, vote4stcharles.net, api.vote4douglas.com, vote4fairfax.com, workerportal.vote4douglas.com, apps.konnech.net, www.vote4douglas.com, www.vote4boston.com, www.vote4ocf.com, indyapi.pollchief.com, api.vote4ocf.com, 365helpdesk.vote4detroit.net, indy.pollchief.com, www.vote4allen.us, resultsadmin.vote4detroit.net, www.vote4fairfax.com ssl.cert.issuer.common_name: Go Daddy Secure Certificate Authority - G2 ssl.cert.sha1_fingerprint: f9:a5:c8:17:8e:5d:d8:7d:e3:ad:99:60:e5:29:a7:83:3e:01:e7:b6 More SSL Details available...

IP	Port	Type	Summary
4.227.233.75 Last Detected: 11/1/22 5:28 AM --	443/tcp	ssl	ssl.cert.subject.organization_name: -- ssl.cert.subject.common_name: lakecounty.pollchief.net ssl.cert.subject_dns: 365helpdesk.vote4detroit.net, api.vote4ocf.com, vote4fairfax.com, api.vote4douglas.com, www.vote4boston.com, signwap.vote4detroit.net, www.vote4douglas.com, www.vote4ocf.com, www.vote4fairfax.com, resultsadmin.vote4detroit.net, apps.konnech.net, workerportal.vote4douglas.com, www.vote4allen.us, lakecounty.pollchief.net, www.lakecounty.pollchief.net ssl.cert.issuer.common_name: Go Daddy Secure Certificate Authority - G2 ssl.cert.sha1_fingerprint: b9:8e:8f:ca:95:c7:09:e3:b0:3c:c2:c5:7d:92:77:5b:90:39:90:b4 More SSL Details available...
75.75.210.254 Last Detected: 11/1/22 4:17 AM --	443/tcp	ssl	ssl.cert.subject.organization_name: -- ssl.cert.subject.common_name: www.vote4stcharles.net ssl.cert.subject_dns: www.vote4stcharles.net, vote4stcharles.net, api.vote4douglas.com, vote4fairfax.com, workerportal.vote4douglas.com, apps.konnech.net, www.vote4douglas.com, www.vote4boston.com, www.vote4ocf.com, indyapi.pollchief.com, api.vote4ocf.com, 365helpdesk.vote4detroit.net, indy.pollchief.com, www.vote4allen.us, resultsadmin.vote4detroit.net, www.vote4fairfax.com ssl.cert.issuer.common_name: Go Daddy Secure Certificate Authority - G2 ssl.cert.sha1_fingerprint: f9:a5:c8:17:8e:5d:d8:7d:e3:ad:99:60:e5:29:a7:83:3e:01:e7:b6 More SSL Details available...

Showing 1 to 3 of 3 entries.

BINARYEDGE

We are a multifunctional team that focus its effort on acquiring, analyzing and classifying internet wide data, by combining efforts in the areas of Cybersecurity, Engineering and Data Science.

Know more about us [here](#).

LINKS

[About Us](#)

[Blog](#)

[Binaryedge.io](#)

[Terms & Conditions](#)

[Documentation](#)

GET IN TOUCH

info@binaryedge.io

support@binaryedge.io

EXHIBIT C

RECEIVED

DEC 22 2022

STATE OF MICHIGAN 30TH CIRCUIT COURT
IN THE CIRCUIT COURT FOR THE COUNTY OF INGHAM

GRANT BRADLEY, individually,

Plaintiff,

v

KONNECH INC,
a Michigan corporation, and
EUGENE J. YU, an individual,

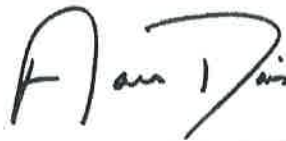
Defendant.

Case No.: 22-0853-CZ

Hon. WANDA M. STOKES

Thaddeus E. Morgan (P47394)
Aaron L. Davis (P77406)
Fraser Trebilcock Davis & Dunlap, P.C.
124 W. Allegan, Suite 1000
Lansing, Michigan 48933
Telephone: (517) 377-0822
adavis@fraserlawfirm.com
Attorneys for Plaintiff

There is no other pending or resolved civil action arising out of the transaction or occurrence alleged in the complaint.



Aaron L. Davis

VERIFIED COMPLAINT AND JURY DEMAND

NOW COMES, Plaintiff, GRANT BRADLEY, by and through his undersigned counsel, FRASER TREBILCOCK DAVIS & DUNLAP, P.C., and for his Verified Complaint against these Defendants, states as follows:

I. NATURE OF THE CASE

1. This is a suit brought under the Michigan Whistleblower Protection Act, MCL § 15.361 *et seq*, or alternatively, a Wrongful Discharge in Violation of Michigan Public Policy. Plaintiff, Grant Bradley (hereinafter “Plaintiff”), was employed as the Implementation Manager with Defendant, Konnech Inc. (hereinafter “Defendant Konnech”) until October 11, 2022, when Defendant terminated his employment as a direct result of Plaintiff’s cooperation with the Los Angeles County District Attorney’s Office, following the arrest of Defendant Eugene J. Yu (hereinafter “Defendant Yu”). Defendant Yu was arrested by Meridian Twp. Police following an investigation by the Los Angeles County District Attorney’s Office that revealed Defendants Konnech and Yu made available poll worker’s private data to foreign nationals working in China in violation of a multi-million dollar contract with Los Angeles County.

2. During his employment, Plaintiff was told by his superiors to say outwardly to customers that poll worker data was not stored overseas, not available to foreign nationals, and that they had no idea why Defendant Yu was arrested. Defendant Yu told Plaintiff not to “worry about” the Chinese nationals working on Defendant Konnech’s software and coding and also claimed companies like Microsoft and Apple had Chinese programmers working on their software behind the scenes.

3. In approximately September 2022, following accusations made by True the Vote, Plaintiff began investigating the extent of the information provided by Defendant Konnech to the programmers based out of Wuhan, China. Plaintiff confirmed that Defendants Yu and Konnech had been providing to these Chinese

programmers private data of poll workers, to include social security numbers and other personal identifying information.

4. Following Defendant Yu's arrest, Plaintiff cooperated with Los Angeles County District Attorney's Office in providing them handwritten notes and other documentation evidencing Defendants' illegal activities. At the Plaintiff's request, the lead investigator from the Los Angeles County District Attorney's office was brought back to the office in order for the Plaintiff to offer additional information for the investigation. In the week between Defendant Yu's arrest (October 4, 2022) and Plaintiff's dismissal (October 12, 2022), Plaintiff was told by other senior level management for Defendant Konnech that he would not have to speak to clients anymore, as Plaintiff proclaimed that he would not lie to the customers about their data not being made available to foreign nationals.

5. Shortly thereafter, Plaintiff was locked out of his business software accounts (October 11, 2022). Additionally, Defendant Konnech maliciously blocked the Plaintiff's payroll account so that the Plaintiff was unable to retrieve personal compensation documentation. He then received an emailed letter from Defendant Konnech's counsel on October 12, 2022 informing him that his position had been eliminated as a result of "current economic conditions and challenges facing the company."

6. Plaintiff's reputation in his chosen field has been ruined by the decision of Defendants to illegally store information on servers housed in China. Plaintiff had

aspirations of running for political office, but has been told by political pundits that he is now “untouchable” due to his employment history with Defendants.

7. Plaintiff brings this lawsuit to address and confront Defendant’s retaliatory behavior.

II. PARTIES

8. Plaintiff, Grant Bradley, is an individual who resides in Ingham County, Michigan. Plaintiff was an employee of Konnech Inc. as its Implementation Manager up until Plaintiff was unlawfully terminated for cooperating with Los Angeles County District Attorney following the arrest of Defendant Yu.

9. Defendant, Konnech Inc., is a Michigan corporation with a principal place of business located at 325 East Grand River, Suite 225, East Lansing, Michigan, 48823.

10. Defendant, Eugene J. Yu, is an individual who, upon information and belief, resides in Ingham County, Michigan. Defendant Yu is the Chief Executive Officer of Defendant Konnech Inc. Defendant Yu was arrested on or about October 4, 2022 by the Meridian Twp. Police Department, following an announcement by the Los Angeles County District Attorney that it had charged him with storing data about poll workers on servers in China.

III. JURISDICTION AND VENUE

11. The amount in controversy is in excess of Twenty-Five Thousand Dollars (\$25,000.00) and is otherwise within the jurisdiction of this Court pursuant to MCL § 600.601 and MCL § 600.605.

12. Venue is proper in this judicial circuit pursuant to MCL § 600.1621.

IV. GENERAL ALLEGATIONS

13. Plaintiff was hired by Defendant Konnech on or about January 19, 2022 for a position to start on March 1, 2022 as a Business Analyst, and was promoted to Implementation Manager in May of 2022.

14. Plaintiff reported to Eric Staats and Luis Nabergoi, but regularly had daily contact and interaction with Defendant Yu.

15. According to its website, Defendant Konnech provides “election logistic software” to its 32 clients it currently serves in North America. Defendant Konnech claims to be “the developers ... the designers ... the coders ... and ... project management experts.” In reality, Defendant Konnech’s developers, designers and coders are all Chinese nationals based out of Wuhan, China.

16. At one point, these Chinese nationals were direct employees of Defendant Konnech. But Defendant Konnech outwardly claimed to terminate the relationship with the Chinese nationals in response to public political pressure to sever ties with China. However, internally, Defendant Yu had no intention of severing the relationship with the Chinese nationals. He hired them back as

independent contractors and assigned to them the exact same responsibilities they held as employees.

17. As further evidence of Defendant Yu's disregard for the laws of this State, shortly after Plaintiff started his employment with Defendant Konnech, Defendant Yu approached Plaintiff about making a campaign contribution to Michigan Secretary of State Jocelyn Benson's campaign in his name that Defendant Konnech would reimburse him for. Plaintiff immediately recognized Defendant Yu's request to be a violation of Michigan Campaign Finance Law and rejected the overture from Defendant Yu.

18. Plaintiff received a promotion to Implementation Manager in May 2022, for which he supervised a team of seven (7) business analysts and four (4) interns. For his efforts, Plaintiff was to make \$80,000 per year and was told to develop a bonus structure for himself and the entire company.

19. Plaintiff's performance during the course of his employment with Defendant Konnech was stellar, as evidenced by the additional responsibilities assigned to the Plaintiff. Plaintiff maintained direct communication with clients across the United States who used Defendant Konnech's products and worked with the Chinese programmers on a daily basis.

20. As part of his employment with Defendant Konnech, Plaintiff witnessed customer's data (specifically poll watcher information) being made accessible to foreign nationals from China. Plaintiff spoke out to his direct supervisors about his concern that these foreign nationals had access to the data and was told that

”everyone [other software companies like Microsoft and Apple] was doing it.” Plaintiff did not know the full extent of the information provided to the Chinese nationals until approximately September 2022 when True the Vote began making allegations against Defendant Konnech.

21. At that time, Plaintiff began to investigate the extent of the information provided to the Chinese programmers by Defendants Yu and Konnech and began researching state and federal laws regarding the sharing of personal identifying information with foreign nationals.

22. Plaintiff recognized that Defendants had been breaking the law for some time and immediately set out to find alternative work. Regrettably, Plaintiff’s efforts to secure alternative work were unsuccessful before the raid by the police.

23. On or about October 4, 2022, police from the East Lansing police department and Los Angeles County District Attorney’s office raided the offices of Defendant Konnech in Okemos and seized company equipment, to include servers and hard drives.

24. Defendant Yu was arrested and charged by the Los Angeles County District Attorney’s Office with illegally storing poll worker data on servers housed in China.

25. Following Defendant Yu’s arrest, Plaintiff was told by his supervisors not to speak with the police or cooperate in their investigation of Defendants Yu and Konnech’s activities.

26. Plaintiff, knowing what Defendant Yu and Defendant Konnech had been engaged in, ignored the directive of his supervisors and asked to meet with the police on the day of the raid so that he could provide them with handwritten notes and other electronic evidence he believes further substantiates Defendants' illegal activities.

27. Thereafter, Plaintiff told his direct reports that he was uncomfortable interfacing with clients on behalf of Defendant Konnech and told his supervisors that he would not tell customers that their data is not stored overseas or not accessible by the Chinese programmers.

28. Following Defendant Yu's arrest and Plaintiff's attestation that he will not lie to customers, supervisors Polcynand Nabergoi told Plaintiff that he would not have to talk to customers anymore.

29. On or about October 7, the Plaintiff spoke with Defendant Yu via Microsoft Teams call. In that call, Defendant Yu congratulated the Plaintiff on his success as the Implementation Manager and spoke extremely favorably about the Plaintiff's team management following the raid.

30. On or about October 11, the Plaintiff asked supervisor, Kelly Shettler, to meet with clients in the Plaintiff's place. As supervisor Shettler was unaware of the Plaintiff no longer speaking with clients, The Plaintiff explained to supervisor Shettler that the Plaintiff would not be interacting with clients for the time being. Within one hour of the communication to supervisor Shettler, the Plaintiff received a call from Defendant Yu terminating his employment. Within days of Plaintiff's decision to cooperate with police and statement that he refused to lie to customers,

Defendants Yu and Konnech locked Plaintiff out of his software and terminated his employment.

COUNT I
VIOLATION OF THE MICHIGAN WHISTLEBLOWERS' PROTECTION ACT
MCL § 15.361 et seq.

31. Plaintiff incorporates by reference paragraphs 1 through 30 of this Verified Complaint.

32. The Michigan Whistleblowers' Protection Act ("WPA"), MCL § 15.362, provides as follows:

An employer shall not discharge, threaten, or otherwise discriminate against an employee regarding the employee's compensation, terms, conditions, location, or privileges of employment because the employee, or a person acting on behalf of the employee, reports or is about to report, verbally or in writing, a violation of a suspected violation of a law or regulation or rule promulgated pursuant to the law of this state, a political subdivision of this state, or the United States to a public body.

(Emphasis added).

33. At all material times, Plaintiff was an employee within the meaning of WPA, MCL § 15.361(a).

34. At all material times, Defendant was Plaintiff's employer within the meaning of the WPA. MCL § 15.361(b).

35. Plaintiff engaged in a protected activity under the WPA by reporting Defendants Konnech and Yu's illegal behavior to police investigators acting on behalf of the Los Angeles County District Attorney's Office.

36. As a direct result of Plaintiff engaging in the protected activity described above, Defendants intentionally discriminated and retaliated against Plaintiff and otherwise violated his rights under the WPA in ways which include, but are not limited to, demanding Plaintiff not cooperate with police or the Los Angeles County District Attorney's Office, locking him out of his work email, and terminating Plaintiff's employment.

37. As a direct and proximate result of Defendants' unlawful actions, Plaintiff sustained damages including, but not limited to, loss of earnings, loss of career opportunities, mental and emotional distress, loss of reputation and esteem in the community, and attorney fees and costs.

COUNT II
IN THE ALTERNATIVE, WRONGFUL DISCHARGE IN VIOLATION OF
MICHIGAN PUBLIC POLICY

38. Plaintiff incorporates by reference paragraphs 1 through 37 of this Verified Complaint.

39. It is Michigan's public policy to promote adherence to state and federal statutes and regulations and it is in the best interest of the State and its citizens to protect and promote compliance with legal authority.

40. It is Michigan's public policy to allow employees to perform their job duties in accordance with the law without fear of retaliation.

41. It is Michigan's public policy to allow employees to express opinions, concerns and complaints to appropriate authorities as to violations of laws and

regulations that they become aware of in the course of performing their job and/or that they are asked to ignore, participate in, or otherwise permit to continue.

42. On October 3, 2022, Defendant Konnech's offices were raided and Defendant Yu was arrested by authorities acting on behalf of the Los Angeles County District Attorney's Office.

43. Plaintiff was told not to speak with the police or cooperate with their investigations of Defendants.

44. Plaintiff spoke with the police investigators and cooperated with providing them handwritten notes supporting the allegations brought against Defendants Konnech and Yu.

45. Plaintiff also told his supervisors that he would not lie to customers that their poll worker data was not being made available to foreign nationals.

46. Defendants Konnech and Yu terminated Plaintiff in retaliation for his opposition to Defendants' illegal directives to not cooperate with the police investigation.

47. Defendants' termination of Plaintiff constituted a violation of Michigan's public policy.

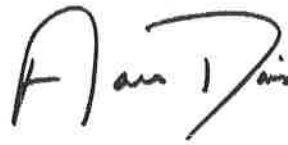
48. As a direct and proximate result of Defendants' unlawful actions, Plaintiff sustained damages including, but not limited to, loss of earnings, loss of career opportunities, mental and emotional distress, loss of reputation and esteem in the community, and attorney fees and costs.

WHEREFORE, Plaintiff requests that this Court enter Judgment in his favor for back wages and fringe benefits, future wages and fringe benefits, damages for the exacerbation of ongoing emotional and mental distress, and attorney fees and costs.

DEMAND FOR TRIAL BY JURY IS HEREBY MADE

FRASER TREBILCOCK

Attorneys for Plaintiff



Dated: December 22, 2022

By: _____
Aaron L. Davis (P77406)
124 West Allegan Street, Suite 1000
Lansing, MI 48933-1736
(517) 482-5800 – Telephone
(517) 482-0887 – Facsimile

VERIFICATION

STATE OF MICHIGAN)
) ss
COUNTY OF INGHAM)

GRANT BRADLEY, being first duly sworn, states as follows:

The information in this Complaint is based on my personal knowledge. I am informed and believe that the matters stated in the Complaint are true and on that basis, I affirm that the information contained in the foregoing is true and correct to the best of my knowledge, information and belief.

Further deponent sayeth not.



GRANT BRADLEY

Subscribed and sworn to before me
this 20th day of December, 2022

Aisa Alfano

Notary Public
Eaton County, Michigan
Acting in Ingham County
My Commission Expires: 12/20/2023

EXHIBIT D

STATE OF MISSOURI

§

ST. LOUIS COUNTY

§

§

AFFIDAVIT OF HARRY HAURY

Before me, the undersigned notary, on this day personally appeared Harry Haury, whose identity is known to me, who under oath states as follows:

1. I am the acting CEO of Cain & Associates. Among many other roles, I have served the National Security Agency and other agencies as a senior information assurance architect. These broad engagements involving development of critical elements of the U.S. National Infrastructure have extended over a period of over 25 years.
2. On October 4, 2022, the Los Angeles County District Attorney started the seizure of Konnech, Inc.'s electronic servers found at its two corporate locations as well as computers, cell phones and external electronic storage devices found at the home of Konnech's CEO, Eugene Yu. The seizure occurred in Michigan in accordance with a lawful search warrant for the headquarters and a criminal complaint against Mr. Yu.
3. Cain & Associates was tasked with assisting the Los Angeles County District Attorney's Office Bureau of Investigation in the execution of the court-ordered search warrant. I coordinated the physical search for the devices, along with Andrew Stevens, LA County's investigator.
4. Based on my experience, Konnech's system of data protection and access amounted to by far the worst example of complete disregard or negligence regarding the protection of PII and sensitive data I have ever seen. We discovered a breach of U.S. data that is classified as a "total loss of control".
5. During our investigation, Cain & Associates:
 - a. confirmed multiple instances of Konnech hosting, on servers based in China, U.S. citizens' personally identifiable information (PII);
 - b. confirmed thousands of instances of Konnech data, including U.S. citizens' PII, and software being transferred to and from China;
 - c. found evidence in Konnech's private company messages that elections software code was being developed, tested, and maintained in China;

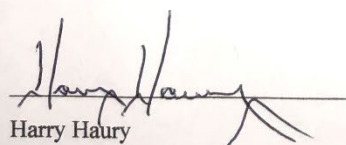
- d. confirmed that Konnech was providing administrative credentials to Chinese developers;
 - e. discovered, more disturbingly, that the Konnech-provided PollChief software used by Los Angeles County (and likely other U.S. jurisdictions) suffered from a security vulnerability that allowed *any* PollChief or Konnech worker to elevate his, her, or own user status to “super user,” giving him or her access to the applications at a privilege above those dictated by security policy which includes broad access to information on all U.S. poll workers in the system;
 - f. obtained evidence that Konnech employees have shared election-related data through, from, and on Chinese servers and applications;
 - g. obtained evidence in downloaded messages that indicated Eugene Yu was involved in developing Chinese government election software; and
 - h. obtained evidence showing Konnech is associated with companies based in mainland China that are subsidized by and have received honors from the Chinese government;
6. I also worked with a confidential informant at the Konnech locations who provided us with usernames and passwords to access various Konnech Internet-connected accounts, such as Jira (used by programmers to report bugs and add software development tasks, or tickets), Konnech’s internal email system, and the China-based collaboration service DingTalk.
 7. However, by about the fourth day following the seizure, someone systematically began shutting off access to these and other accounts, one by one. On information and belief, the restriction of the DA’s access was orchestrated by either Konnech, Inc. or by persons or entities in China with whom Konnech was associated, including any of the many super users on the accounts.
 8. Since becoming aware of Konnech’s breach of PII, we have been in contact with the DCSA and law enforcement in counties that are customers of Konnech, including Allegheny County, PA; Fairfax County, VA; DeKalb County, GA; and Johnson County, KS.
 9. I asked these customers if Konnech had notified them of any data breach, as it is obligated to do, and every person to whom I spoke said that Konnech had given them no

such notification. There is no option but to conclude Konnech has violated its duty to disclose to its customers, the affected counties and municipalities, the PII breach.

10. We concluded that this incident is a very high risk indicator of an intrusion by a foreign intelligence into the U.S. strategic infrastructure, and as obliged by law, we informed the Defense Counterintelligence and Security Agency (DCSA) and other pertinent law enforcement agencies of this contact.
11. My recommendation is that the seized devices be placed into the temporary custody of an independent forensic examiner to be mirror-imaged. The critical issue is for independent cyber recovery from the equipment to be conducted by one, or more, qualified teams using FBI/DOJ standard recovery techniques either bonded or under affiant pledges.
12. The level of recovery is best if the original equipment is used. The next best would be making bit-by-bit full disk images. The least optimal would be making copies of relevant files. Chain of custody may be maintained by using digital hashes. The parties could then have their own cyber analysis performed using their respective copies. Placing all raw material under a non-disclosure order or appropriate seal would serve to ensure an intact repository to support current and future investigations.
13. On information and belief, and subject to change upon receipt of chain of custody and other information, the list of seized devices includes but is not limited to those in Exhibit F.

I certify under penalty of perjury that the foregoing is true and correct.

Further Affiant Sayeth Not.


Harry Haury

Subscribed to and sworn before me on this ____ day of February, 2023.

BETHANY HARMON
Notary Public - Notary Seal
Franklin County - State of Missouri
Commission Number 22987422
My Commission Expires Oct 11, 2026

Bethany Harmon

Notary Public in and for the state of Missouri

EXHIBIT E

STATE OF Nevada
Clark COUNTY

§
§
§

AFFIDAVIT OF BRIAN GLICKLICH

Before me, the undersigned notary, on this day personally appeared Brian Glicklich, whose identity is known to me, who under oath states as follows:

1. At approximately 6:30AM Pacific Time on Sunday November 6th, 2022, I received a call from a man identifying himself as Peter McAllister, who said he had been until recently the general manager of Konnech Australia. A Peter McAllister was indeed listed on the website at <https://www.konnech.com.au/About.html>, which is now no longer active but may be found at www.archive.org. I made contemporaneous notes of the call.

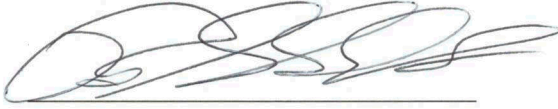
2. Mr. McAllister indicated that he had seen my appearance on War Room the day before and had information relevant to the imprisonment of Catherine Engelbrecht and Gregg Phillips, following a contempt proceeding, that he wanted to convey to me.

3. Mr. McAllister told me that on Monday October 10th, someone had started deleting Konnech company emails from a website in Vietnam. McAllister believed these actions to be at the instigation of Eugene Yu, the CEO of Konnech, Inc. McAllister said he had received this information from Konnech's CTO, a man named Luis Nabergoi Puente, who was based in Barcelona. Luis had contacted McAllister via WhatsApp. Mr. McAllister told me that Luis had indicated to him that the emails being deleted were all those that had a TXT or JSON attachment. Mr. McAllister said that Luis's interpretation was that someone at Konnech intended to get rid of any emails with log files attached that may have gone to China. Further, Mr. McAllister indicated that Mr. Yu's nephew, a man named Jun Yu, was removing all apps in Konnech's internal messaging application called DingTalk.

4. Mr. McAllister indicated that Eugene's brother runs a company that provides similar election software to the Chinese Communist party. Mr. McAllister also said that he had been asked by Mr. Yu to sell that same software in Australia. Mr. McAllister said he had recently been asked to resign, by Mr. Yu, ostensibly in order to help fund Eugene Yu's litigation.

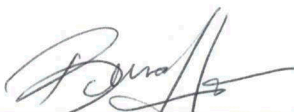
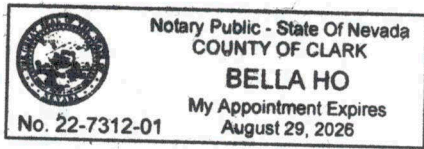
I certify under penalty of perjury that the foregoing is true and correct.

Further Affiant Sayeth Not.



Brian Glicklich

Subscribed to and sworn before me on this 24 day of February, 2023.



Notary Public in and for the state of NV