UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

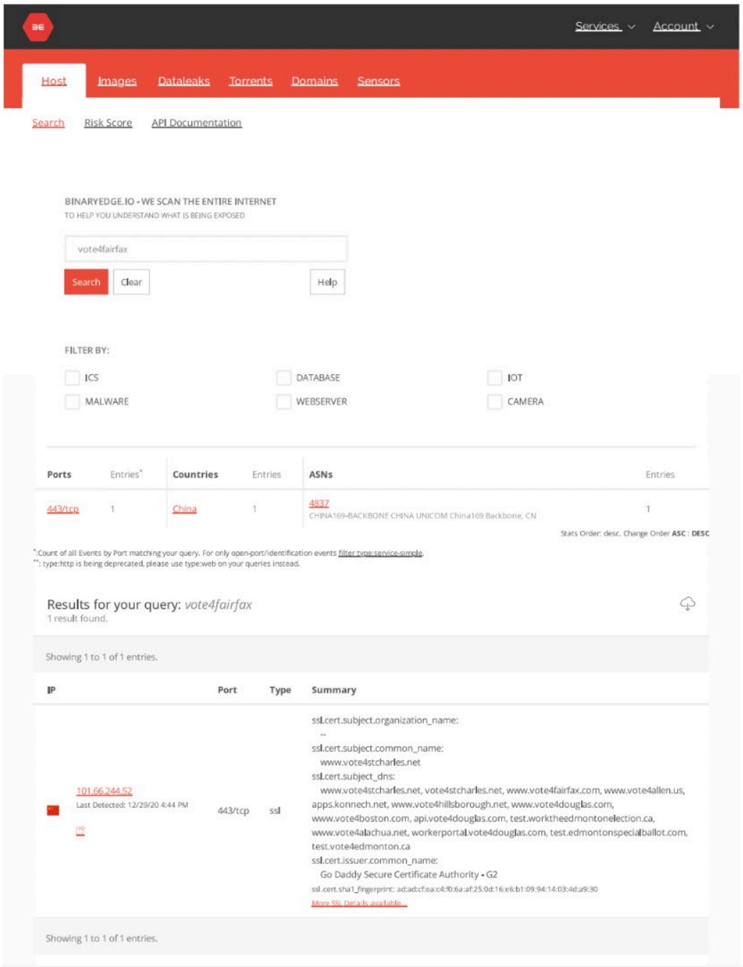
KONNECH, INC.,	§	
	§	
Plaintiff,	§	Civil Action No. 4:22-cv-03096
	§	
v.	§	
	§	
TRUE THE VOTE, INC., *et al.,*	§	
	§	
Defendants.	§	

DEFENDANTS' OPPOSED EMERGENCY MOTION FOR LEAVE TO INSPECT PROPERTY OF PLAINTIFF TO PREVENT FURTHER SPOLIATION 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":



BINARYEDGE.IO - WE SCAN THE ENTIRE INTERNET
TO HELP YOU UNDERSTAND WHAT IS BEING EXPOSED

vote4fairfax

FILTER BY:

□ ICS □ DATABASE □ IOT
□ MALWARE □ WEBSERVER □ CAMERA

Ports	Entries*	Countries	Entries	ASNs	Entries
443/tcp	1	China	1	4837 CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN	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*
1 result found.

Showing 1 to 1 of 1 entries.

IP	Port	Type	Summary
🟥 101.66.244.52 Last Detected: 12/29/20 4:44 PM	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, www.vote4fairfax.com, www.vote4allen.us, apps.konnech.net, www.vote4hillsborough.net, www.vote4douglas.com, www.vote4boston.com, api.vote4douglas.com, test.worktheedmontonelection.ca, www.vote4alachua.net, workerportal.vote4douglas.com, test.edmontonspecialballot.com, test.vote4edmonton.ca ssl.cert.issuer.common_name: Go Daddy Secure Certificate Authority - G2 ssl.cert.sha1_fingerprint: ad:ad:cf:ea:c4:f0:6a:af:25:0d:16:e6:b1:09:94:14:03:4d:a9:30 More SSL Details available...

Showing 1 to 1 of 1 entries.

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. 118CV03305TWPDML, 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-image[3] 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 following[4]:

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