

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

KONNECH, INC.,

PLAINTIFF,

v.

**TRUE THE VOTE, INC., GREGG
PHILLIPS, and CATHERINE
ENGELBRECHT,**

DEFENDANTS.

§
§
§
§
§
§
§
§
§
§
§

CIVIL ACTION NO. _____

PLAINTIFF’S ORIGINAL COMPLAINT

TO THE HONORABLE UNITED STATES DISTRICT JUDGE:

COMES NOW, Plaintiff Konnech, Inc. (“Konnech”), in the above styled cause, and files this Original Complaint, and would respectfully show the Court as follows:

INTRODUCTION

1. Defendants True the Vote, Inc., its founder and President Catherine Engelbrecht, and board member Gregg Phillips (“Defendants”) have intentionally, repeatedly, and relentlessly attacked Konnech and its founder Eugene Yu with Defendants’ unique brand of racism and xenophobia by their completely baseless claims that Konnech, its founder, and employees are “Chinese operatives,” who are spearheading a “Red Chinese communist op run against the United States,” that Konnech is tied to the Confucius Institute, which Defendants say is part of the Chinese Communist Party, that Konnech was the subject of a long-running FBI counterintelligence investigation, that Konnech obtained contracts with certain U.S. city and county voting districts after bribing public officials, and that the Chinese Communist Party is somehow controlling U.S. elections through Konnech because its founder and some of its employees are of Chinese descent. Defendants’ false accusations of treason, espionage, bribery, and election fraud, which they peddle

to enrich themselves at Konnech's expense, are completely fabricated and constitute defamation *per se*.

2. The truth is that Konnech is a U.S. company founded and operated by a U.S. citizen who has no affiliation with the Chinese Communist Party whatsoever. Konnech obtains its contracts through transparent public government bidding processes, and has never engaged in bribery or any other criminal activity of any sort. All of Konnech's U.S. customer data is secured and stored exclusively on protected computers located within the United States. Konnech's software products are not involved in any way in the registration of voters, the production, distribution, scanning, or processing of ballots, or the collection, counting or reporting of votes. Indeed, Konnech never handles any ballots and no ballots or other voting counts ever enter any of Konnech's computer servers. It thus begs the question how Defendants could believe that Konnech could ever be involved in election fraud—or how it otherwise could have helped “steal” the 2020 Presidential Election from former President Donald Trump—when Konnech has had no involvement with ballots in any U.S. election. But the simple matter is, Defendants have no regard for the truth or the consequences of their actions, because the truth would not profit them.

3. Indeed, Defendants are in business to capitalize from their claim that the 2020 Presidential Election was “stolen.” Defendants Phillips and Engelbrecht have been referred to as the “Bonnie and Clyde” of election fraud¹, and they have enriched themselves by spreading conspiracy theories, which they present as factual in nature, about the 2020 Presidential Election, largely funded by money funneled through Defendant True the Vote, which some commentators

¹ See Mimi Swartz, *How True the Vote Fabricates Claims of Election Fraud, for Fun and Profit*, Texas Monthly (Aug. 22, 2022), available at, <https://www.texasmonthly.com/news-politics/true-the-vote-election-fraud/>.

have called a “big grift.”² Defendants were in fact the subject of a suit filed in 2020 by a conservative megadonor, who, after speaking with Defendant Engelbrecht, donated \$2.5 million to help fund Defendant True the Vote’s efforts to fight election fraud. The donor later discovered, however, that his money was instead siphoned through Defendant True the Vote, and other entities established by Defendants Phillips and Engelbrecht, for their own personal gain.³

4. Defendants most recently capitalized on their claims of election fraud through their involvement in the production of a so-called “documentary” titled *2000 Mules* in which they sought to convince their followers that people, who they refer to as “mules,” were paid to collect and deposit fake ballots into ballot boxes for the 2020 Presidential Election which they contend changed its outcome. The theories peddled in *2000 Mules*, however, have been repeatedly disproven.⁴ Apparently realizing that their *2000 Mules* tale had run its course, Defendants Phillips

² See Cassandra Jaramillo, *She Helped Create the Big Lie. Records Suggest She Turned It Into a Big Grift*, *Reveal News* (June 8, 2022), available at, <https://revealnews.org/article/true-the-vote-big-lie-election-fraud/>.

³ See *Eshelman v. True the Vote, Inc., OSPEC Group, LLC, Engelbrecht, Bopp, Jr., Phillips, and The Bopp Law Firm*, 4:2020-cv-04034, filed November 25, 2020 in the U.S. District Court for the Southern District of Texas; see also Richard Salame, *Was Election Denial Just a Get-Rich-Quick Scheme? Donors’ Lawsuits Look for Answers* (Feb. 6, 2021), available at, <https://www.typeinvestigations.org/investigation/2021/02/06/was-election-denial-just-a-get-rich-quick-scheme-donors-lawsuits-look-for-answers/>.

⁴ See *Fact Check-Does ‘2000 Mules’ provide evidence of voter fraud in the 2020 U.S. presidential election?*, *Reuters* (May 27, 2022), available at, <https://www.reuters.com/article/factcheck-usa-mules-idUSL2N2XJ0OQ>; *FACT FOCUS: Gaping Holes in the Claims of 2k Ballot ‘Mules’*, *Associated Press* (May 3, 2022), available at, <https://www.usnews.com/news/politics/articles/2022-05-03/fact-focus-gaping-holes-in-the-claim-of-2k-ballot-mules>; Tom Dreisbach, *A pro-Trump film suggests its data are so accurate, it solved a murder. That’s false*, *NPR* (May 17, 2022), available at, <https://www.npr.org/2022/05/17/1098787088/a-pro-trump-film-suggests-its-data-are-so-accurate-it-solved-a-murder-thats-fals>; Phillip Bump, *Even the geolocation maps in ‘2000 Mules’ are misleading*, *The Washington Post* (May 19, 2022), available at, <https://www.washingtonpost.com/politics/2022/05/19/even-geolocation-maps-2000-mules-are-misleading/>.

and Engelbrecht declared an end to “mules” at an August 2022 True the Vote, invitation-only event which they called “The Pit.”

5. The Pit, they promised, would be the event where Defendants would finally release “devastating information” that would definitively prove the 2020 U.S. Presidential election was stolen. Instead, Defendants used The Pit as a platform to announce their website, and publicly launch their attack against Konnech by spreading baseless lies.

6. In an attempt to bolster their false accusations, Defendants claim that they have obtained financial and other sensitive personal data of 1.8 million U.S. poll workers—including social security numbers, phone numbers, email addresses, and banking information—from Konnech’s protected computers. As an initial matter, Konnech has never managed customer data for that many poll workers or even a small percentage of that many poll workers. But regardless, based on the extensive security measures Konnech has in place, Defendants could only access *any* of Konnech’s data if they illegally hacked into and stole data from Konnech’s protected computers.

7. Defendants have in fact portrayed their access to Konnech’s protected computers as unauthorized. Defendant Phillips specifically described on a recent podcast how Defendant Engelbrecht had an idea and asked him to look into Konnech’s election software, how he then traveled to a Dallas, Texas hotel room to meet his “analysts,” how they put “towels under the doors” in an effort to conceal their knowingly unlawful conduct, and then how “analysts,” who were acting at his direction, successfully hacked into Konnech’s servers and unlawfully downloaded its data. Defendants even admit *they* are now the subject of an ongoing FBI investigation due to their misconduct targeting Konnech. But apparently undeterred, Defendants

have continued their attacks on Konnech and have publicly and repeatedly declared their intent to release the information they stole from Konnech's servers.

8. Defendants have pushed their false narrative with social media posts that “ReTruth” (the Truth Social equivalent of a Retweet on Twitter) conspiracy theories published by armchair “experts” and anonymous sources. Defendants lead a chorus of online adherents who are encouraged by Defendants—through social media postings and podcast appearances—to engage in further attacks against Konnech. Numerous conspiracy theories attempting to affiliate Konnech with the Chinese Communist Party have appeared online since The Pit. To be clear, Konnech, a previously relatively unknown entity, has gone viral since The Pit, with countless Tweets and Truth Social postings using the #Konnech hashtag. But the consequences of Defendants' actions are far more serious in that Defendants' public smear campaign has resulted in repeated death threats against Konnech's founder and his family which have forced them out of their home in fear for their lives.

9. Defendants' allegation that a vast international conspiracy concerning the U.S. Presidential Election would be ignored by the Federal Government—and, in fact, concealed by the FBI—but proven by conspiracy theorists and con artists using basic internet searches and posts on social media, demonstrates Defendants' recklessness and disdain for the truth.

10. Defendants know what they are doing is wrong, and have tried, in vain, to avoid responsibility for their misconduct by encouraging and using others to perform their dirty work for them. But Defendants have already gone too far, and they cannot avoid liability for their own misconduct and for masterminding this entirely fabricated conspiracy against Konnech.

11. Absent intervention of this Court, such damaging behavior will continue to occur, which is particularly problematic in light of the upcoming 2022 midterm elections, for which

Konnech has contracts to provide election logistics software for voting districts across the country. Konnech thus files this action to recover damages as a result of Defendants' defamatory statements, and interference with Konnech's current and prospective business relationships, and seeks a restraining order to immediately and permanently restrain Defendants and those acting in concert with them from accessing, obtaining, using and/or disclosing any data from Konnech's protected computers.

PARTIES

12. Plaintiff Konnech, Inc. is incorporated in Michigan and headquartered in East Lansing, Michigan.

13. Defendant True the Vote, Inc. is a Texas Nonprofit Corporation which is headquartered in Houston, Texas, at 18720 FM 249, Suite A, Houston, Texas 77070, and can be served through its registered agent, Registered Agents, Inc., at 5900 Balcones Drive, Suite 100, Austin, Texas 78731, or wherever else it may be found.

14. Defendant Catherine Engelbrecht resides at 13909 Track Rd. East, Cat Spring, Texas 78933, and can be served at said address or wherever else she may be found.

15. Defendant Gregg Phillips resides at 1752 Coates Pass, Birmingham, Alabama 35244, and can be served at said address or wherever else he may be found.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1331, because Konnech has asserted claims against Defendants under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq.* This Court also has supplemental jurisdiction over Konnech's state law claims pursuant to 28 U.S.C. § 1367(a). This Court further has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(a), because the parties have diversity of citizenship and the amount in controversy exceeds \$75,000.

17. Venue is proper in the Southern District of Texas (Houston Division) because a substantial part of the events giving rise to the claims occurred in Houston, Texas where Defendant True the Vote is headquartered and Cat Spring, Texas where Defendant Engelbrecht resides, and a substantial part of the property that is the subject of the action is situated in Houston, Texas and/or Cat Spring, Texas. Additionally, venue is proper in the Southern District of Texas (Houston Division) because Defendants and, in particular, Defendants Engelbrecht and True the Vote, have published defamatory statements that are the subject of this action from within the Southern District of Texas (Houston Division).

18. This Court has personal jurisdiction over Defendant True the Vote because it is incorporated in Texas and has its principal place of business in Texas. This Court has personal jurisdiction over Defendant Engelbrecht because she is domiciled in Texas. This Court has personal jurisdiction over Defendant Phillips because he availed himself of the benefits and protections of the laws of the State of Texas by, among other things, committing a tort and other unlawful misconduct against Konnech while in Texas. Specifically, Defendant Phillips, while acting in concert with Defendants Engelbrecht and True the Vote, has admitted that he obtained confidential information and data from Konnech's protected computers while located in Texas, and obtained data from Konnech's protected computers while located in Texas which has also been provided to Defendant True the Vote which is headquartered in Houston, Texas.

FACTUAL BACKGROUND

Konnech, Inc.

19. Konnech, Inc. is a U.S. company which is incorporated in Michigan and was founded by its President and CEO, Eugene Yu, who is a U.S. citizen. Mr. Yu built Konnech on his own from the ground up. Konnech provides governmental entities in the U.S. with an election logistics software product called PollChief which those governmental entities use to recruit, train

and schedule poll workers; coordinate the distribution of equipment and supplies to polling places; and dispatch support personnel to address technical and other issues. Konnech does not select, communicate, or otherwise interface with any poll workers. And Konnech's software products are not involved in any way in the registration of voters, the production, distribution, scanning, or processing of ballots, nor the collection, counting or reporting of votes. Indeed, Konnech never handles any ballots and no ballots or other voting counts ever enter any of Konnech's computer servers.

True the Vote's "The Pit" Event

20. In the summer of 2022, Defendants advertised an event they dubbed "The Pit," scheduled for August 13, 2022, at which they claimed they would disclose "devastating" information that would be definitive proof that the 2020 Presidential Election was stolen from former President Donald Trump.

21. The Pit was hosted by Defendants and attended by over 100 by-invitation-only guests who were handpicked by Defendants Engelbrecht and Phillips based on who they believed would be supportive of their conspiracy and who would best spread the disinformation they planned to disclose. The Pit was also livestreamed on Right Side Broadcasting Network.

22. The event featured many different speakers, including Defendants Engelbrecht and Phillips, and served as a pep rally for election fraud conspiracy theorists in anticipation of the 2022 midterm elections. But the main attraction for The Pit was the supposed proof that Defendants claimed they planned to disclose, which was not part of *2000 Mules*, but, in their words, would serve as definitive proof that the 2020 Presidential election was a sham.

23. While The Pit was still livestreaming, Defendants Phillips and Engelbrecht took the stage to finally make the big announcement. The announcement, however, was nothing more than

an advertisement for a website Defendants created, where Defendants claim their subscribers can log on and view the purported evidence of election fraud.

The Pit Livestream is Turned Off

24. Upon information and belief, and according to social media posts from those in attendance at The Pit, Defendants turned off the livestream and then disclosed to attendees that they had been secretly working on something they called “The Tiger Project”—which is the code name and hashtag for their campaign against Konnech—during which they sent dozens of FOIA requests to Konnech’s customers, all in an apparent effort to intimidate those customers or to otherwise raise customers’ suspicions about Konnech. But even more shocking, Defendants falsely claimed that they discovered that Konnech had an unsecured server located in Wuhan, China, which Defendants hacked into and stole data from. Specifically, Defendants claimed to have illegally downloaded from Konnech’s server personal data on 1.8 million U.S. poll workers, which they claim is a vehicle for the Chinese Communist Party to breach U.S. elections.



25. To be clear, however, all of Konnech’s U.S. customer data is secured and stored exclusively on protected computers located within the United States. Konnech controls access to its offices, enters into confidentiality agreements with its customers and employees, and uses two-

factor authentication, restricted access, and other security measures to control access to its protected computers. Only a select group of Konnech employees that have been provided with that two-factor authentication have authority to access the protected computers which contain poll worker data.

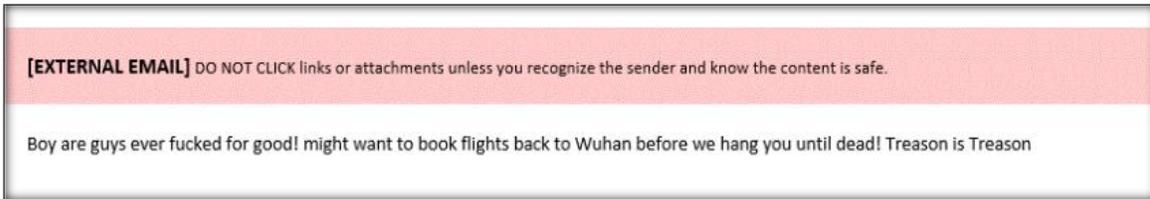
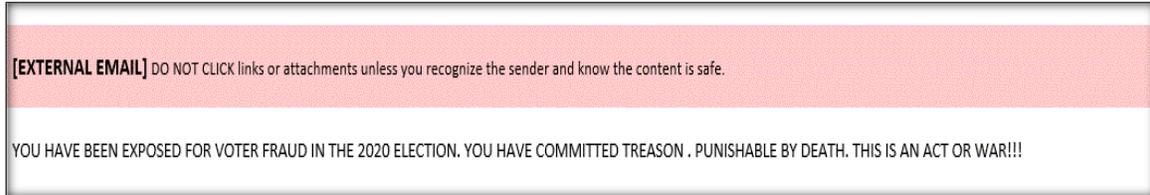
26. Defendants additionally claimed that they brought all of their information to the FBI and made a formal complaint. Unsurprisingly, Defendants sought to capitalize on certain public sentiment against the FBI on the heels of the recent raid on Mar-a-Lago, and claimed that the FBI turned the tables on them, and began an investigation of *Defendants* for hacking Konnech's protected computers and stealing its data.

27. Then, to ensure maximum damage from their defamatory statements, Defendants encouraged The Pit attendees, as documented in the following social media post, to spread what they learned at the event, to do their own research on Konnech, to publish their findings on the internet and, moreover, to continue attacking Konnech:



And as things typically evolve with the internet in the 21st century, the conspiracy theory and attacks against Konnech—all of which were initiated by Defendants at The Pit—quickly spread, and the previously relatively unknown Konnech went viral.

28. Sadly, as a foreseeable consequence of Defendants’ malicious and baseless attacks against Konnech, Mr. Yu has been the target of repeated death threats, which have forced him and his family to leave their home in fear for their lives:

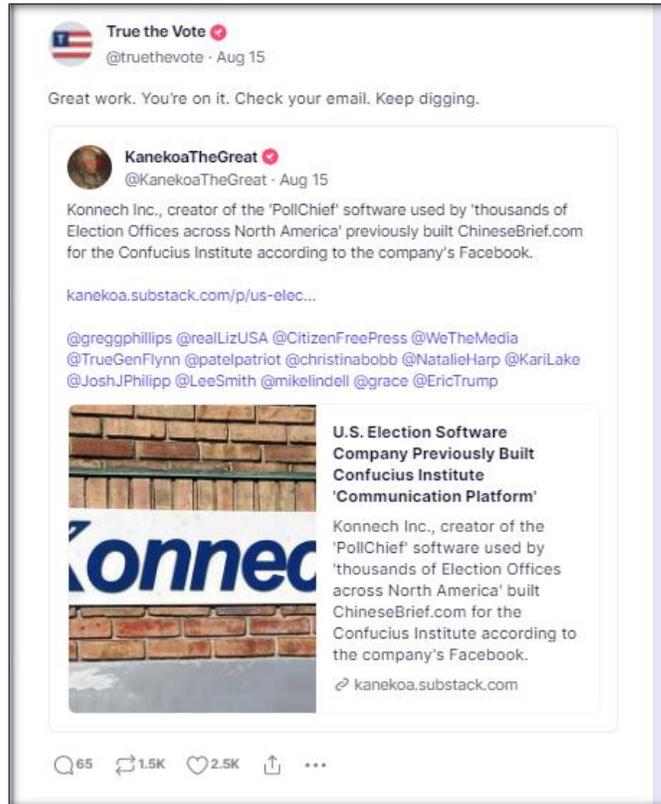


Defendants Continue to Defame Konnech

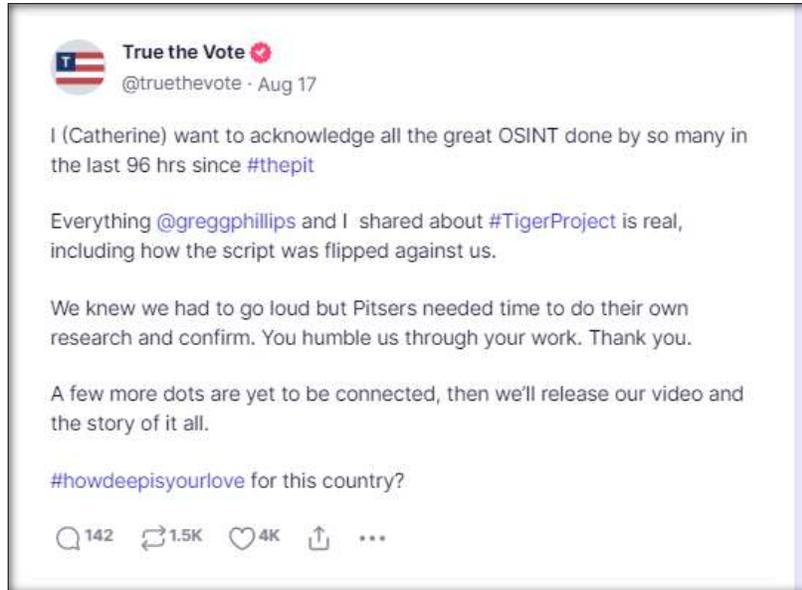
29. Following The Pit, Defendants went on a media blitz to publicize their newly fabricated conspiracy theory in an unabashed effort to enrich themselves at the expense of Konnech, all under the guise of being “Patriots” who are supposedly uncovering election fraud—which one can supposedly learn about, but only by subscribing to Defendants’ various web-based platforms.

30. Defendants have further perpetuated their attacks by posting and ReTruthing articles of purported research compiled by anonymous posters which associate Konnech to everything from Mark Zuckerberg, to George Soros, the Chinese Communist Party, and even the origins of COVID-19.

31. As one example of many, on August 15, 2022, True the Vote posted an article which falsely claims, among other factually incorrect assertions, that Konnech built software for the Confucius Institute, an organization which they claim is linked to the Chinese Communist Party, and further encouraged its followers to “keep digging.”:



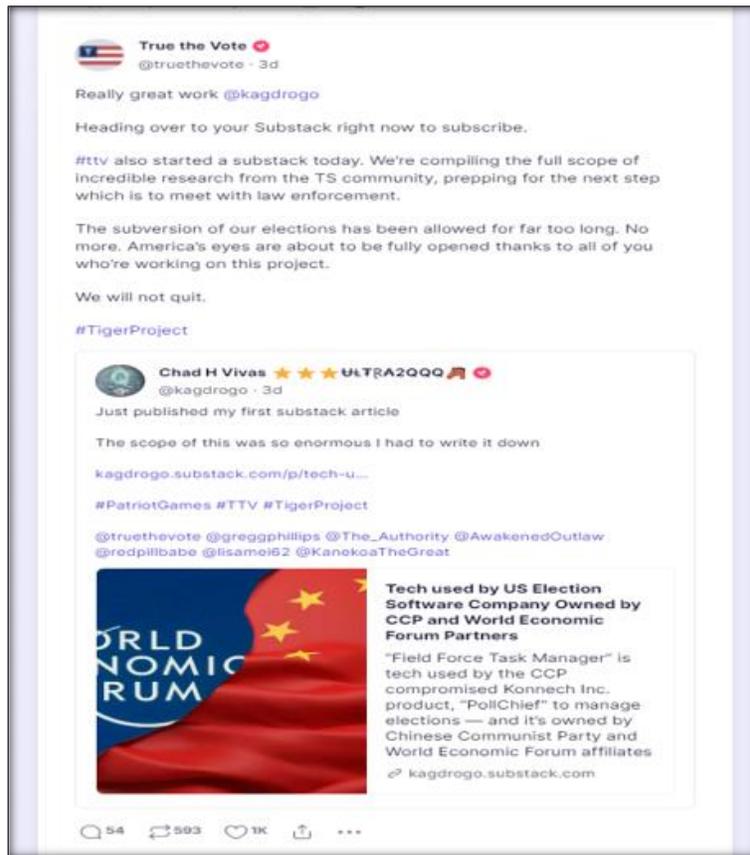
32. On August 17, 2022, True the Vote posted to Truth Social representing that everything they said at The Pit was a factual matter and, again, encouraged others to continue to research Konnech and further expand the ever-growing conspiracy theory:



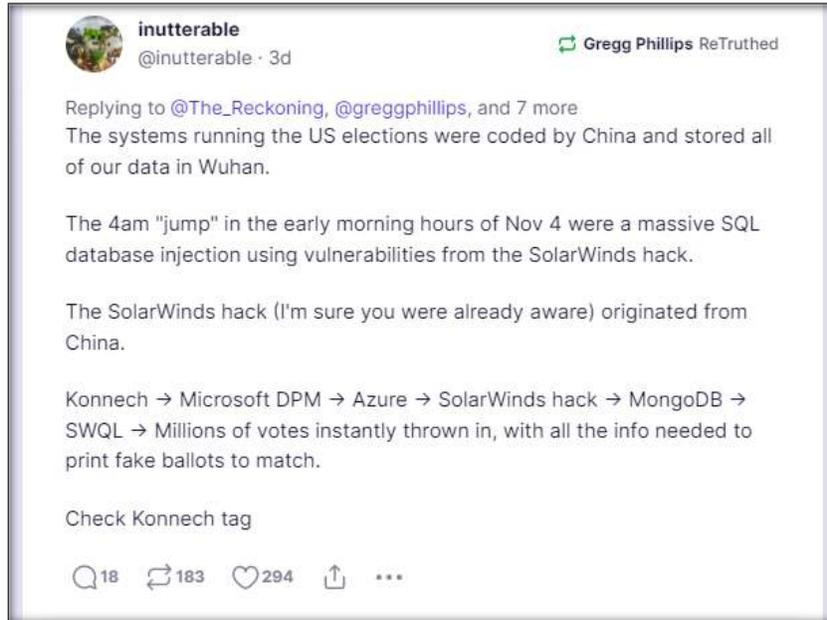
33. On August 21, 2022, True the Vote directly accused Konnech of unlawful acts in connection with a government contract and handling of ballots, even though Konnech has never handled ballots in any U.S. election:



34. On August 27, 2022, True the Vote posted an article claiming that Konnech is “owned by the Chinese Communist Party,” even though Konnech is owned by U.S. citizens who are not affiliated with the Chinese Communist Party, and claiming that Konnech is involved in the “subversion of our elections” which is tantamount to falsely accusing Konnech of election fraud, treason, and espionage:



35. On August 26, 2022, Defendant Phillips also ReTruthed allegations that Konnech is directly connected to a “jump” of votes for President Biden even though Konnech has never handled ballots in any U.S. Election:



36. On September 5, 2022, True the Vote hosted a “Q&A” podcast concerning their “Tiger Project,” which claimed to be an event where Defendants would reveal “How the CCP is Breaching US Elections.” The podcast, however, merely summarized the same baseless rhetoric against Konnech, and Defendants did not produce any evidence to support their baseless accusations:



37. And on September 8, 2022, Defendant Phillips ReTruthed an article claiming that the “FBI Conceals Chinese Infiltration of U.S. Election Software,” and quotes a prior statement by Phillips that “[t]his is a red Chinese communist op run against the United States by Chinese operatives and it’s a disaster”:



38. Defendants’ attacks on Konnech, however, are not just limited to social media postings. Defendants—who constantly seek publicity—have also made numerous appearances on their own and others’ podcasts where they have further spewed and perpetuated their lies about Konnech and, in fact, repeatedly confessed to hacking Konnech’s protected computers and stealing its data.

Defendants Falsely Accuse Konnech of Bribery

39. For example, Defendants have falsely accused Konnech of bribing the City of Detroit to obtain a contract simply by making campaign contributions of an unstated amount. Specifically, on an August 15, 2022 podcast titled “Devolution Power Hour – Gregg Phillips

Interview,” Defendant Phillips (pictured below on the right) falsely implied that Konnech only received its contract with Detroit because Konnech bribed the officials there: “The two biggest donations . . . were from, guess who, Konnech. And then all of a sudden, they get, they get this fast ballot counting software contract and, and next thing, you know, the election counting stops[.]” But, as explained throughout, Konnech does not, and has never, performed any ballot counting, scanning, or processing in any U.S. election. And Konnech has never engaged in bribery of any form and a legal campaign contribution, if any, is not a bribe.



Defendants Falsely Accuse Konnech of Maintaining Unsecure Chinese Servers and Admit to Hacking and Stealing Konnech’s Data

40. Defendants have also falsely accused Konnech of maintaining unsecure Chinese servers for their election logistics software and, in the process, admit to hacking and stealing Konnech’s data. For example, on an August 23 podcast titled “Prophets and Patriots,” Defendant Phillips described meeting his “guys” at a hotel room in Dallas, where they put “towels under the doors” like “some kind of a James Bond kind of thing,” and proceeded to hack into a Konnech server. Indeed, Defendant Phillips admitted on that podcast that “[w]e took [Konnech’s data]

directly” and that Defendant True the Vote plans to publicly “release all of [Konnech’s] data” through “drops” to subscribers of Defendants’ website.

41. Defendant Phillips repeated these claims on an August 30, 2022 podcast titled, “Here’s How They’ll Try to Steal the Midterms,” where Phillips described, once again, traveling to Dallas, Texas to meet his so-called “analysts,” where they “plugged one of their computers into the television” and began “scrolling through millions and millions of records about Americans,” all of which he claims to have obtained by gaining unauthorized access to Konnech’s protected computers. Defendant Phillips also described how he “immediately drove down to Houston” and got Defendant Engelbrecht “to come over and meet [him]” that next morning, where they came up with a plan to file a complaint with the FBI and turn over the data they stole.

42. Likewise, on a September 2, 2022 podcast hosted by Defendant Phillips called “Patriot Games”—during which he admits the FBI accused him of being “the thief that stole the Chinese internet”—Defendant Engelbrecht (pictured below on the right) confessed to how Defendants conspired to unlawfully access Konnech’s protected computers, and how she and True the Vote “pulled in [Defendant Phillip’s] team, and asked them to take a deeper dive” around the security of Konnech’s software. Defendant Phillips told The Pit attendees that they accessed Konnech’s alleged Chinese server by using a password after finding vulnerabilities in the server.



Defendants Falsely Claim Konnech is the Subject of a Long-Running FBI Investigation

43. Additionally, Defendants have falsely claimed that Konnech is the subject of a long-running FBI investigation, and that a grand jury indictment against Konnech is imminent. Specifically, during the “Prophets and Patriots” podcast, Defendant Phillips claimed to have been “involved in a major and mature counterintelligence operation with the FBI” investigating Konnech.

44. And during the “Patriot Games” podcast, Defendants claimed that they are working with people “to bring this work to, to a grand jury for the first time,” and that they have the “support of, of a major prosecutorial office in the United States . . . and [that] they are moving this along,” thus further claiming, as a factual matter, that Konnech has committed unlawful acts worthy of prosecution.

45. But contrary to these unfounded accusations, Defendants admit *they* are the ones who are the subject of an ongoing FBI investigation, which they have freely and repeatedly admitted (if not boasted about) at the Pit and in each podcast on which they appear.

Defendants Falsely Accuse Konnech of Storing U.S. Poll Worker Data on Chinese Servers

46. Further, Defendants have falsely accused Konnech of storing sensitive and personal data—including social security numbers, email addresses, phone numbers, and banking information—on 1.8 million U.S. poll workers on servers in China, and otherwise running their election logistics application through Chinese servers. For example, on an August 31, 2022 podcast called “Stealing the Chinese Internet w/ Gregg Phillips of 2000 Mules,” Defendant Phillips falsely claimed that he found an “unbelievable amount of data from a US company run by a Chinese national . . . Yeah, the CCP. We later found out that there’s all kinds of data on this server.

There's, there's data from counties all over the United States where the servers installed, there's all sorts of other related software.”

47. And during the September 5, 2022 “Tiger Project” podcast advertised by Defendants, 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. Similarly, on the “Here’s How They’ll Try to Steal the Midterm” podcast mentioned above, Defendant Phillips falsely claimed that Konnech’s election software “apps were running from China, the database is running in China. It’s on the Chinese internet, meaning the Chinese own it.”

49. And on the “Prophets and Patriots” podcast mentioned above, Defendant Phillips falsely claimed that Konnech has “done military ballots,” and has “online voting systems that they’ve created,” and that they were all “created by Chinese programmers[.]”

50. But the truth of the matter is, all of Konnech’s U.S. customer data is secured and stored exclusively on protected computers located within the United States. Konnech does not, and has never, stored any actual customer or poll worker data on any server in China as Defendants falsely claim. Konnech does not, and has never, performed any ballot counting, scanning, or processing in any U.S. election. And furthermore, Konnech has never managed customer data for 1.8 million poll workers, or even a small fraction of that number, despite Defendants’ claiming to find 1.8 million U.S. poll worker records on a Konnech server in China.

Defendants Falsely Accuse Konnech of Being a Vehicle for the Chinese Communist Party

51. Moreover, Defendants have maliciously and dangerously claimed that Konnech and its founder and CEO are members of and, in fact, spies for the Chinese Communist Party, who are using Konnech to spy and commit fraud in connection with U.S. elections.

52. During the “Prophets and Patriots” podcast, Defendant Phillips claimed that Konnech, through its alleged Chinese Communist affiliates, “pulled this [election fraud] off on the United States.”

53. And during the “Tiger Project” podcast, Defendants Phillips and Engelbrecht made further absolutely baseless and defamatory allegations against Konnech by expressly claiming that “these are Chinese operatives in the United States,” and that “this is a, a Red Chinese communist op run against the United States by Chinese operatives, and it’s, it’s a disaster.”

54. To set the record straight, neither Konnech, nor its founder and CEO, have any affiliation with the Chinese Communist Party. Konnech is not a “Chinese operative,” and Konnech is not used by the Chinese Communist Party for any purpose, whatsoever.

55. Defendants’ statements have been made with actual malice, knowing or reckless disregard for the truth, including intentional lies concerning their possession of evidence of fraud or meddling by the Chinese Communist Party that simply does not exist. Defendants have further manufactured, misrepresented and cherry-picked information available on the internet to draw unsubstantiated connections to support their false accusations. They have purposely avoided or intentionally disregarded publicly available evidence, facts, and reliable resources rebutting and disproving their false claims. And they have formed and stuck to a false preconceived narrative in spite of the facts, by relying on and putting forward facially unreliable and anonymous sources, all in a plan to enrich themselves.

56. Defendants have perpetuated their claims after being put on notice of the falsity of their accusations. They have ignored former President Donald Trump’s own Attorney General William Barr—the former chief law enforcement officer of the United States Federal Government—who has repeatedly declared that there was no evidence of voter fraud to overturn

the 2020 Presidential Election.⁵ And moreover, the notion that a vast international conspiracy concerning the U.S. Presidential Election would be ignored by the Federal Government—and, in fact, concealed by the FBI—but proven by conspiracy theorists and con artists using basic internet searches and posts on social media, demonstrates Defendants’ recklessness and disdain for the truth.

Defendants Intentionally Interfere with Konnech’s Business Relationships and Konnech Suffers Harm

57. Unfortunately, although Defendants live in a world of make believe which they have created for the sole purpose of enriching themselves, their actions have real world consequences, including substantial harm to Konnech and its business reputation that has been built over decades, but is at risk of being destroyed by Defendants’ baseless lies.

58. For example, on August 27, 2022, an anonymous poster on Truth Social posted the name and email address of the board members of DeKalb County, Georgia’s Board of Registration & Elections, and a Konnech contract proposal for DeKalb County, and encouraged followers to contact the board members because the board was considering using Konnech for their voter software. The post was ReTruthed at least 246 times and, just a few days later, Defendant Phillips “Truthed” about DeKalb County, and posted the same Konnech contract proposal that the anonymous source posted. Defendant Phillips’s actions are thus directly intended to damage Konnech’s business relationships.

59. Indeed, ever since Defendants’ attacks on Konnech began, Konnech has had to perform additional, costly security audits, and spent time and money investigating Defendants’

⁵ See Michael Balsamo, *Disputing Trump, Barr says no widespread election fraud*, AP News (June 28, 2022), available at, <https://apnews.com/article/barr-no-widespread-election-fraud-b1f1488796c9a98c4b1a9061a6c7f49d>.

hacking, and to ensure that it has no security breach. Additionally, Defendants' conduct demonstrates their intent to prevent Konnech from developing business relationships with other prospective governmental entities in the U.S., apparently solely on the basis that Konnech has employees of Chinese descent. Defendants' conduct is not only damaging to Konnech, it also deters other would-be election logistic companies from entering the market—or will cause other such companies to shutter—without which, elections would be unmanageable for cities and counties, leading to further election integrity issues.⁶

60. Absent intervention from this Court, Konnech believes that Defendants will continue its campaign to destroy Konnech's current and prospective business relationships, Defendants will make continued efforts to hack and otherwise compromise Konnech's protected computers, Defendants will continue their possession of data that they claim they stole from Konnech, and Defendants will publicly disclose the data they stole.

61. Defendants' conduct is all a calculated effort to intentionally inflict substantial harm to Konnech and its business, including harm to its reputation, customer confidence, and goodwill, and to impugn the integrity of U.S. elections.

CLAIM 1: DEFAMATION, LIBEL, AND SLANDER

62. Konnech repeats and realleges the allegations in paragraphs 1 through 61, as if fully set forth herein.

63. Defendants published the foregoing statements of purported fact referring to

⁶ For example, conspiracy theorists have recently caused one Texas county's entire elections department to resign. *See Neil Vigdor, 3 Election Officials Resigned in a Texas County*, The New York Times (Aug. 18, 2022), available at, <https://www.nytimes.com/2022/08/18/us/politics/texas-gillespie-elections-threats.html>; *see also* Michael Murney, *Anti-flouride conspiracists harassed Texas county election workers until they all quit*, MSN (Aug. 29, 2022), available at, <https://www.msn.com/en-us/news/us/anti-flouride-conspiracists-harassed-texas-county-election-workers-until-they-all-quit/ar-AA11fir2>.

Konnech.

64. The foregoing statements by Defendants were false in their particular details and their gist and essence in the entire context in which they were made.

65. The foregoing statements by Defendants were defamatory, libelous and slanderous (collectively, “defamatory” or “defamation”) and in making the statements, Defendants acted with actual malice, with knowledge of the falsity of the defamatory statements, or at least with reckless disregard of their falsity by purposely avoiding the truth, making inherently improbable assertions and, in fact, lying about Konnech’s commission of what are serious crimes in the United States.

66. The foregoing statements by Defendants were not privileged.

67. The foregoing statements by Defendants constitute defamation *per se* in that they falsely state that Konnech committed the crimes of treason, espionage, bribery and election fraud, and in that they plainly accuse Konnech of breaking the law.

68. The foregoing defamatory statements by Defendants have injured Konnech’s reputation and exposed Konnech to public hatred, animus, contempt or ridicule, or financial injury. These false statements were made to impeach Konnech’s honesty, integrity, virtue, or reputation and thereby expose it to financial injury. The defamatory statements are therefore defamatory *per se*.

69. A reasonable reader would understand that all of the foregoing statements referred to Konnech because, among other things, they referred to it by name, nickname, affiliation, or the name of their “Tiger Project,” which is specifically directed at and targets Konnech.

70. Defendants are strictly liable for the damages caused by their defamatory statements. Alternatively, Defendants were negligent with respect to the truth or falsity of the defamatory statements of purported fact. Alternatively, Defendants knew and know that the

defamatory statements of fact were false, or were reckless with regard to whether the statements of purported fact were false.

71. As a result of Defendants' defamatory statements, Konnech suffered pecuniary injury and damages are presumed.

CLAIM 2: TORTIOUS INTERFERENCE WITH EXISTING AND PROSPECTIVE BUSINESS RELATIONS

72. Konnech repeats and realleges the allegations in paragraphs 1 through 71, as if fully set forth herein.

73. Defendants willfully and intentionally interfered with the existing and/or prospective business relationships of Konnech.

74. Konnech has many existing contracts with various governmental entities in the U.S. which retain Konnech to provide election logistic software.

75. Defendants have contacted Konnech's customers in an effort to cause them to breach or cancel contracts with Konnech. Defendants have further encouraged others to contact Konnech's customers in an effort to cause those customers to breach or cancel contracts with Konnech.

76. Konnech has suffered damages as a proximate result of Defendants' misconduct as Konnech's current customers have required Konnech to undergo costly audits that would not have been requested but for Defendants' actions.

77. There is also a reasonable probability that Konnech would have entered into additional business relationships with other governmental entities in the U.S. but for Defendants' actions.

78. Defendants have acted willfully and intentionally to prevent those business relationships from occurring by way of their independently tortious acts, which began with their

defamation and violation and conspiracy to violate the federal Computer Fraud and Abuse Act and the Texas Harmful Access by Computer statute, and the disclosure of information stolen from Konnech's servers.

79. Upon information and belief, Konnech has suffered damages as a result of Defendants' interference.

**CLAIM 3: VIOLATION OF THE COMPUTER FRAUD AND
ABUSE ACT, 18 U.S.C. § 1030**

80. Konnech repeats and realleges each allegation in paragraphs 1 through 79, as if fully set forth herein.

81. Konnech's computers are used in interstate and/or foreign commerce or communication in the course of Konnech's business and therefore are "protected computers" under the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030(e)(2)(b-c).

82. Konnech's protected computers are secured by numerous security features, including two-factor authentication which is only provided to select Konnech employees.

83. Defendants admit to intentionally accessing Konnech's protected computers without authorization, and as a result of such conduct, caused Konnech damage and loss.

84. Defendants, by, among other things, knowingly disclosed, or otherwise have threatened to disclose, the information stolen from Konnech's protected computers, knowingly caused the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caused damage to Konnech's protected computers.

85. As a result of Defendants' aforementioned unauthorized access to Konnech's protected computers, Konnech has suffered loss in an amount to be proven at trial, well in excess of \$5,000, which includes, but is not limited to, investigating, and assessing the need to remediate

Defendants' unauthorized access, and responding to the attacks and assessing the damage, if any, caused to Konnech's protected computers by Defendants.

86. Additionally, Defendants knowingly caused damage to Konnech's protected computers, by, among other things, impairing the integrity of Konnech's protected computers, and intentionally stealing data and information contained on a Konnech server.

87. Konnech has suffered further injury and harm in the loss of confidential and protected personal identifying information which was misappropriated by Defendants, and damage to its reputation and the confidence of its customers.

88. Defendants' misconduct constitutes a violation of the federal Computer Fraud and Abuse Act, 18 U.S.C. *et. seq.*, and Konnech is entitled to damages under the Act.

CLAIM 4: CONSPIRACY TO VIOLATE THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030

89. Konnech repeats and realleges each allegation in paragraphs 1 through 88, as if fully set forth herein.

90. Konnech's protected computers are used in interstate and/or foreign commerce or communication in the course of Konnech's business and therefore are "protected computers" under the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030(e)(2)(b-c).

91. Konnech's protected computers are secured by numerous security features, including two-factor authentication which is only provided to select Konnech employees.

92. Defendants admit to conspiring to intentionally access Konnech's protected computers without authorization and obtaining information from Konnech's protected computers.

93. Defendants admit to conspiring to intentionally access Konnech's protected computers without authorization, and as a result of such conduct, caused Konnech damage and loss.

94. Defendants, by, among other things, knowingly conspired to disclose, or are otherwise knowingly conspiring to disclose, the information stolen from Konnech's protected computers, knowingly caused the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caused damage to Konnech's protected computers.

95. Specifically, Defendants admit they were part of a group who gained unauthorized access to Konnech's protected computers.

96. Defendants admit the objective of their group was to accomplish the violation of the federal Computer Fraud and Abuse Act, by way of gaining unauthorized access to Konnech's protected computers and obtaining and disseminating information taken from those protected computers.

97. Defendants admit to a meeting of the minds to violate the federal Computer Fraud and Abuse Act by way of gaining unauthorized access to Konnech's protected computers and obtaining and disseminating information taken from those protected computers.

98. Defendants committed overt acts to further the objective of their conspiracy by taking actions to gain unauthorized access to Konnech's protected computers and obtaining and disseminating information taken from those protected computers.

99. As a result of Defendants' aforementioned conspiracy to gain unauthorized access to Konnech's protected computers, Konnech has suffered loss in an amount to be proven at trial, well in excess of \$5,000, which includes, but is not limited to, investigating, and assessing the need to remediate Defendants' unauthorized access, and responding to the attacks and assessing the damage, if any, caused to Konnech's protected computers by Defendants.

100. Additionally, Defendants conspired to knowingly cause damage to Konnech's protected computers, by, among other things, impairing the integrity of Konnech's protected

computers, and intentionally stealing data and information contained on Konnech's protected computers.

101. Konnech has suffered further injury and harm in the loss of confidential and protected personal identifying information which was misappropriated by Defendants, and damage to its reputation and the confidence of its customers.

102. Defendants' misconduct constitutes a conspiracy to violate the federal Computer Fraud and Abuse Act, 18 U.S.C. *et. seq.*, and Konnech is entitled to damages under the Act.

CLAIM 5: HARMFUL ACCESS BY COMPUTER, TEXAS CIVIL PRACTICE & REMEDIES CODE § 143.001; TEXAS PENAL CODE § 33.02

103. Konnech repeats and realleges the allegations in paragraphs 1 through 102, as if fully set forth herein.

104. Konnech maintains "computers," "computer networks," and/or "computer systems" (hereinafter, collectively "computers"), as those terms are defined in TEXAS PENAL CODE § 33.01.

105. Konnech's computers are secured by numerous security features, including two-factor authentication which is only provided to select Konnech employees.

106. Defendants admit to intentionally or knowingly accessing Konnech's computers without the effective consent of Konnech, and as a result of such conduct, caused Konnech damage and loss.

107. As a result of Defendants' access to Konnech's computers without effective consent, Konnech has suffered damages in an amount to be proven at trial, which includes, but is not limited to, investigating, and assessing the need to remediate Defendants' unauthorized access, and responding to the attacks and assessing the damage, if any, caused to Konnech's computers by Defendants.

108. Defendants knowingly and intentionally caused damage to Konnech's computers, by, among other things, impairing the integrity of Konnech's computers, and knowingly and intentionally stealing data and information contained on a Konnech computer.

109. Konnech has suffered further injury and harm in the loss of confidential and protected personal identifying information which was misappropriated by Defendants, and damage to its reputation and the confidence of its customers.

110. Defendants' misconduct constitutes a violation of TEXAS PENAL CODE § 33.02, which may be brought as a civil action pursuant to TEX. CIV. PRAC. & REM. CODE § 143.001.

**CLAIM 6: CONSPIRACY TO GAIN HARMFUL ACCESS BY COMPUTER,
TEXAS CIVIL PRACTICE & REMEDIES CODE § 143.001; TEXAS PENAL
CODE § 33.02**

111. Konnech repeats and realleges the allegations in paragraphs 1 through 110, as if fully set forth herein.

112. Konnech maintains "computers," "computer networks," and/or "computer systems" (hereinafter, collectively "computers"), as those terms are defined in TEXAS PENAL CODE § 33.01.

113. Defendants admit to conspiring to intentionally access Konnech's computers without effective consent and obtaining information from Konnech's computers.

114. Defendants admit to conspiring to intentionally access Konnech's computers without effective consent, and as a result of such conduct, caused Konnech damage and loss.

115. Specifically, Defendants admit they were part of a group who gained access to Konnech's computers without effective consent.

116. Defendants admit the objective of their group was to gain access to Konnech's computers without effective access, and obtaining and disseminating information taken from those computers.

117. Defendants admit to a meeting of the minds to gain access to Konnech's computers without effective consent, and obtaining and disseminating information taken from those computers.

118. Defendants committed overt acts to further the objective of their conspiracy by taking actions to gain access to Konnech's computers without effective consent and obtaining and disseminating information taken from those computers.

119. As a result of Defendants' aforementioned conspiracy to gain access to Konnech's computers without effective consent, Konnech has suffered damages in an amount to be proven at trial, which includes, but is not limited to, investigating, and assessing the need to remediate Defendants' unauthorized access, and responding to the attacks and assessing the damage, if any, caused to Konnech's computers by Defendants.

120. Additionally, Defendants conspired to knowingly cause damage to Konnech's computers, by, among other things, impairing the integrity of Konnech's computers, and intentionally stealing data and information contained on Konnech's computers.

121. Konnech has suffered further injury and harm in the loss of confidential and protected personal identifying information which was misappropriated by Defendants, and damage to its reputation and the confidence of its customers.

122. Defendants' misconduct constitutes a conspiracy to violate TEXAS PENAL CODE § 33.02, which may be brought as a civil action pursuant to TEX. CIV. PRAC. & REM. CODE § 143.001.

CLAIM 7: CONVERSION

123. Konnech repeats and realleges the allegations in paragraphs 1 through 122, as if fully set forth herein.

124. Defendants currently possess data owned or legally possessed by Konnech, or to which Konnech otherwise has an entitlement to possession.

125. Defendants unlawfully and without authorization assumed and exercised dominion and control over the property to the exclusion of, or inconsistent with Konnech's rights as owner of the property, which removed the need for Konnech to demand the return of the property. However, Konnech demanded the return of the data Defendants claim to have taken and Defendants did not return it.

126. Defendants' actions were intentional, malicious, oppressive, or fraudulent, and give rise to liability for exemplary damages according to proof at trial.

127. As remedies for Defendants' conversion, Konnech seeks compensatory and exemplary damages, a constructive trust over the converted materials, and an injunction requiring Defendants to return the converted materials to Konnech.

**CLAIM 8: VIOLATION
OF THE TEXAS THEFT LIABILITY ACT**

128. Konnech repeats and realleges the allegations in paragraphs 1 through 127, as if fully set forth herein.

129. Konnech had the possessory right to property taken from its protected computers by Defendants.

130. Defendants unlawfully appropriated the property Konnech had a possessory right to through its business as an election logistics software company.

131. Defendants' misappropriation of Konnech's property was and is willful and malicious because they intentionally tried to steal Konnech's property as a means to enrich themselves by peddling disproven conspiracy theories.

132. Defendants' conduct constitutes a violation of the Texas Theft Liability Act, Chapter 134 of the Texas Civil Practice and Remedies Code.

133. As remedies for Defendants' theft, Konnech seeks compensatory and exemplary damages, a constructive trust over the stolen materials, costs and reasonable and necessary attorneys' fees, and an injunction requiring Defendants to return the stolen materials to Konnech.

CLAIM 9: INJUNCTIVE RELIEF

134. Konnech repeats and realleges the allegations in paragraphs 1 through 133, as if fully set forth herein.

135. As set forth in the Third, Fourth, Fifth, and Sixth Causes of Action, *supra*, Defendants have admitted to violating and conspiring to violate the federal Computer Fraud and Abuse Act, 18 U.S.C.A., *et. seq.* and the Texas Harmful Access by Computer statute. There is thus a strong likelihood that Konnech will succeed on its claims in this action.

136. Defendants' misconduct has caused, and continues to cause, Konnech injury including, without limitation, irreparable harm for which there is no adequate remedy at law.

137. There is no adequate remedy at law to compensate Konnech for the irreparable harm caused by the interference with its control and the integrity of its protected computers, the harm to Konnech's reputation, customer confidence, and goodwill it has suffered and will continue to suffer due to Defendants' hacking of Konnech's protected computers and the disclosure of information obtained therefrom. And there is no adequate remedy at law to compensate Konnech for the prior and continued hacking of Konnech's protected computers.

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

139. The balance of equities strongly favors issuing injunctive relief in favor of Konnech as Defendants will suffer no hardship from being ordered to cease and desist from committing continued unlawful acts and, specifically, from gaining unauthorized access to Konnech's protected computers, and to return the data that belongs to Konnech, but was stolen by Defendants.

140. An injunction will not adversely affect the public interest. Rather, an injunction will benefit the public interest because the public has an interest in preventing conduct which the United States Congress and Texas Legislature has determined is unlawful, and an interest in maintaining the integrity of U.S. elections.

JURY DEMAND

Konnech demands a trial by jury.

PRAYER FOR RELIEF

Plaintiff Konnech, Inc. prays that Defendants True the Vote, Inc., Gregg Phillips, and Catherine Engelbrecht be cited to appear and answer herein, and that Konnech, Inc. recover judgment from Defendants as follows:

- a. For a temporary restraining order, preliminary injunction and/or permanent injunction enjoining Defendants, directly or indirectly, and whether alone or in concert with others:
 - i. from accessing or attempting to access Konnech's protected computers;
 - ii. to return to Konnech all property and data obtained from Konnech's protected computers, whether original, duplicated, computerized, handwritten, or any other form whatsoever;
 - iii. from using, disclosing, or exploiting the property and data downloaded from Konnech's protected computers;
 - iv. to preserve, and not to delete, destroy, conceal or otherwise alter, any files or other data obtained from Konnech's protected computers;
 - v. to identify each individual and/or organization involved in accessing Konnech's protected computers;
 - vi. to confidentially disclose to Konnech how, when, and by whom Konnech's protected computers were accessed; and
 - vii. to identify all persons and/or entities, in Defendants' knowledge, who have had possession, custody or control of any information or data from Konnech's protected computers;
- b. Compensatory and exemplary damages in an amount to be determined at trial, constituting its losses from Defendants' misconduct;
- c. A constructive trust for the return of Konnech's stolen and converted property;
- d. Reasonable and necessary attorneys' fees;
- e. Pre- and post-judgment interest at the maximum rate allowed by law;
- f. All costs of suit; and
- g. All such other and further relief, both general and special, at law or in equity, to which Konnech may show itself to be justly entitled or as this Court may deem appropriate.

Dated: September 12, 2022

KASOWITZ BENSON TORRES LLP

By: /s/ Constantine Z. Pamphilis

Constantine Z. Pamphilis

Attorney in Charge

Texas State Bar No. 00794419

SDTX Bar No. 19378

DPamphilis@kasowitz.com

Nathan W. Richardson

Texas State Bar No. 24094914

SDTX Bar No. 24094914

NRichardson@kasowitz.com

1415 Louisiana Street, Suite 2100

Houston, Texas 77002

(713) 220-8800

(713) 222-0843 (fax)

Attorneys for Plaintiff Konnech, Inc.