June 4, 2020

The Honorable Kathy Jennings
Office of the Attorney General
Delaware Department of Justice
Carvel State Building
820 N. French St.
Wilmington, DE 19801

Dear Attorney General Jennings:

We write to urge you to initiate an investigation into the voting system vendor Voatz to determine whether Voatz has abused its corporate charter through deception, misrepresentation, or fraud in a manner that warrants charter forfeiture under 8 Del. Code § 284.[1]

Voatz is a Boston-based startup company that is developing and aggressively marketing an internet-based voting system that enables voters to cast a ballot from an application loaded on to their mobile phones. Over multiple election cycles, Voatz contracted with at least five jurisdictions between four states to provide internet voting systems to voters eligible under the Uniformed and Overseas Citizen Absentee Voting Act (UOCAVA) for local and state-wide elections.

Despite multiple warnings from leading cybersecurity and voting security experts, third-party auditors, and senior federal government officials,[2] Voatz continued to hold out its voting platform as safe, claiming that ballots cast on its platform could not be deleted or altered,[3] and publishing materials and presentations[4] promising

---

[1] Free Speech For People is a non-profit, non-partisan public interest legal organization that works to renew our democracy and our United States Constitution for the people. As part of our mission, we are committed to promoting, through legal actions, secure, transparent, trustworthy and accessible voting systems for all voters.

[2] Maya Kosoff, "A Horrifically Bad Idea: Smartphone Voting is Coming Just in Time for the Midterms," *Vanity Fair,* August 7, 2018; Dr. David Jefferson, et al, "What We Don't Know About the Voatz "Blockchain" Internet Voting System," May 1, 2019. *Available at: https://cse.sc.edu/~buell/blockchain-papers/documents/WhatWeDontKnowAbouttheVoatz_Blockchain_.pdf.*

[3] Robert Hackett, "Denver and West Virginia Deserve Praise for Voting on Blockchain," *Fortune,* March 23, 2019. *Available at: https://fortune.com/2019/03/23/blockchain-vote-election-denver-west-virginia-voatz/*

[4] https://blog.voatz.com/wp-content/uploads/2019/02/West-Virginia-Mobile-Voting-White-Paper-NASS-Submission.pdf

that Voatz's system was robustly vetted and secure.[5] Using these misrepresentations, Voatz contracted to provide internet voting services with the State of West Virginia; Utah County, Utah; Jackson County and Umatilla County, Oregon; and the City of Denver, Colorado. If its technology is more widely adapted, Voatz's insistence that it provides a product with "military grade security"[6] and its continuous refusal to confront its platform's major flaws could have devastating effects on the legitimacy of our elections and jeopardize our national identity as a democracy.

Multiple state and local officials praised Voatz at conferences, media appearances, and interviews, and often through press releases issued from Voatz's sponsor, Tusk Philanthropies. These endorsements were subsequently picked up and amplified through the media:

- Utah's Lieutenant Governor personally vouched for Voatz's security, saying, "I am thrilled that Utah County is partnering with Tusk Philanthropies, Voatz and the National Cybersecurity Center to bring these secure, blockchain-based voting options to Utahns overseas for the upcoming municipal election;"[7]
- Oregon's Deputy Secretary of State Rich Vial proclaimed that "[b]y enabling these voters to cast a ballot using their mobile device which adds the security of modern smartphone technology combined with the security of the blockchain, we can make it easier, and at the same time more secure, for them to cast a ballot from wherever they are in the world;"[8]
- Denver County's Deputy Director of Elections Jocelyn Bucaro praised Voatz, saying, "We are very excited about the promise of this technology. Our goal was to offer a more convenient and secure method for military and overseas citizen voters to cast their ballots, and this pilot proved to be successful."[9]

---

[5] Voatz, "Frequently Asked Questions," https://www.voatz.com/faq.html

[6] Voatz, "Military-Grade Security, Easy To Use: Elections Technology & Civic Engagement," https://freespeechforpeople.org/wp-content/uploads/2020/04/Voatz_1Pager.military.grade_.pdf

[7] "Mobile Voting is Coming to Utah County Municipal Elections," Tusk Philanthropies, July 23, 2019. *Available at: https://www.prnewswire.com/news-releases/mobile-voting-is-coming-to-utah-county-municipal-elections-300889121.html*

[8] "Mobile Voting is Coming to local Oregon Elections," Tusk Philanthropies, Oct. 16, 2019. *Available at: https://www.prnewswire.com/news-releases/mobile-voting-is-coming-to-local-oregon-elections-300939320.html*

[9] "National Cybersecurity Center Successfully Completes Third Party Security Audit for Denver's Mobile Voting Pilot," Tusk Philanthorpies, Aug. 05, 2019. *Available at: https://www.prnewswire.com/news-releases/national-cybersecurity-center-successfully-completes-third-party-security-audit-for-denvers-mobile-voting-pilot-300896234.html*

The combined force of these statements from a wide array of election officials indicates Voatz's campaign to persuade government officials that its system is secure was fruitful. However, evidence has shown that Voatz's claims are spurious and its system does not warrant this confidence. Security studies have established that Voatz's system is vulnerable to foreign hacking and undetectable ballot tampering, and it provides no reliable method of auditing the results of the election.[10] Despite these documented security flaws, Voatz groundlessly rejected this evidence and has failed to satisfactorily remedy its vulnerabilities.

I. The Corporate Charter in Delaware is a privilege subject to revocation in cases of abuse.

Many of the world's largest corporations have availed themselves of the benefits of corporate charters granted by the people and the General Assembly of Delaware. Although Delaware welcomes these businesses, all parties are fully aware that the corporate form and its protections are a privilege, not a right. The Attorney General has the power to request the revocation of a corporate charter by the Court of Chancery for its "abuse." 8 Del. Code § 284. Where there is a "clear case of abuse of corporate privileges and franchises … courts will not hesitate to pass the [corporate death] sentence." *Southerland v. Decimo Club, Inc.*, 16 Del. Ch. 183, 199, 142 A. 786, 793 (1928) (internal citation omitted).

Although what constitutes "abuse" of a corporate charter is underdefined, the general policy, as set by the General Assembly of Delaware by passing multiple consumer protection laws,[11] is that even inadvertent corporate deception—let alone intentional deception, like Voatz's—brings consequences.[12] A corporation should not be permitted to abuse its corporate charter by blatantly deceiving election officials and the voters of multiple states into believing their internet elections are completely secure without consequences. And while Voatz's false and misleading statements may not be within the reach of Delaware's consumer protection laws, they may be in violation of other similarly situated laws.[13] Given the General

---

[10] https://blog.trailofbits.com/2020/03/13/our-full-report-on-the-voatz-mobile-voting-platform/

[11] *See* Consumer Fraud Act, 6 Del. Code § 2511 *et seq.*; Uniform Deceptive Trade Practices Act, 6 Del. Code § 2531 *et seq.*

[12] *See* Olha N.M. Rybakoff, *An Overview of Consumer Protection and Fair Trade Regulation in Delaware*, 8 DEL. L. REV. 63, 68 – 74 (2005).

[13] *See, e.g.*, West Virginia Consumer Protection Act, W. Va. Code §§ 46A-6-101 *et seq.* (prohibiting "unfair, deceptive, and fraudulent acts," *id.* at § 46A-6-101); Utah Code §§ 13-11a-1 *et seq.* (preventing "deceptive, misleading, and false advertising practices and forms in Utah," *id.* at § 13-11a-1); Unlawful Trade Practices Act, Or. Rev. Stat. § 646.607; Colorado Consumer Protection Act; Colo. Rev. Stat. §§ 6-1-101 *et seq.*

Assembly's clear policy statement against deception of purchasers, Delaware should not be providing corporate privileges and legal cover to an entity determined to misrepresent its product in disregard of many states' laws.

In *Young v. Nat'l Ass'n for the Advancement of White People*, 35 Del. Ch. 10, 109 A.2d 29 (1954), the Chancery Court stated, "there is no question but that this Court will forfeit a corporate charter where the abuse of its privileges and franchises is clear." 109 A.2d at 31.[14] Voatz, by grossly misrepresenting the security of its platform and vulnerability to foreign attack, poses a significant threat to the elections of several jurisdictions, and, if allowed to continue abusing its corporate privileges, may soon threaten the legitimacy of our national elections as well.

II. Voatz continues to fundamentally misrepresent the security of its platform and its vulnerability to foreign attack.

Though Voatz's faulty advertisements regarding security successfully persuaded election officials in many states, Voatz's failure to substantiate any of its statements bred distrust. In November 2019, U.S. Senator Ron Wyden (OR) sent a request to the Department of Defense and the National Security Agency asking both to conduct a security evaluation of Voatz, writing:

"*While Voatz claims to have hired independent security experts to audit the company, its servers and its app, it has yet to publish or release the results of those audits or any other cybersecurity assessments. In fact, Voatz won't even identify its auditors. This level of secrecy hardly inspires confidence."*[15]

Senator Wyden followed up in February 2020 with a letter to ShiftState Security, a firm that Voatz had identified as having conducted a security audit of its system, requesting a copy of the evaluation:

"*To convince state and local officials to take a chance on Voatz's controversial technology, Voatz touted an audit conducted by ShiftState Security. ShiftState and Voatz have not published the audit, and Voatz has refused to provide me with a*

[14] The Chancery Court declined to grant the Attorney General's motion for a preliminary injunction, despite the defendant corporation's efforts to undermine Delaware's education laws, because—among other factors—there was "no imminent threat of activities designed to bring about violations of the State election laws." *Id.* at 32.

[15] *Available at*: *https://www.washingtonpost.com/context/sen-ron-wyden-d-ore-letter-regarding-voatz/e9e6dd4f-1752-4c46-8e37-08a0f21dd042/*

copy. However, in a press interview last year, you declared that "Voatz did very well" in the full security review that you and your team conducted."[16]

The ShiftState report has still not been released.

In February of this year, election officials and the public had their first look at Voatz's security from an independent third party when researchers at the Massachusetts Institute of Technology (MIT) published a report that contradicted much of Voatz's claims. The report was a stunning catalogue of security gaps and documented multiple vulnerabilities "that allow different kinds of adversaries to alter, stop, or expose a user's vote."[17]

By reverse engineering the publicly available Voatz mobile application, the MIT researchers were able to analyze and identify several opportunities to compromise, corrupt or alter votes cast over the Voatz application before the ballot even enters the blockchain. The MIT researchers were able to circumvent Voatz's malware protections with "minimal effort," allowing an attacker to corrupt the Voatz application and undetectably alter or spy on vote choices. The researchers also found that votes cast on the application are not loaded directly onto the blockchain; instead they first pass through a server which is also vulnerable to multiple attacks that could manipulate or delete votes making any public audit of votes recorded on the blockchain meaningless.

In addition to documenting multiple, significant vulnerabilities with the Voatz mobile voting system, the MIT researchers included in the appendices a catalogue of eleven of Voatz's published security claims, annotated by the researchers with findings from their research that contradict each claim.[18] This list provides a preliminary foundation to establish that Voatz's security claims are faulty.

Concerned the vulnerabilities could have national security implications, the MIT researchers reached out to the Cybersecurity Infrastructure and Security Agency (CISA) at the Department of Homeland Security (DHS) to share their findings. CISA found the research credible and facilitated communication between the researchers and Voatz to responsibly disclose the security issues to Voatz before

---

[16] *Available at: https://www.wyden.senate.gov/imo/media/doc/022120%20Wyden%20Letter%20To%20Shiftstate%20Security%20RE%20Voatz.pdf*

[17] Michael Spector, James Koppel, Daniel Weitzner, "The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections," Massachusetts Institute of Technology, February 2020.

[18] *Ibid.*

the report was made public. CISA also arranged calls between the MIT researchers and several affected election officials to alert them to the findings.

Voatz responded to the MIT researchers' findings forcefully; staunchly denying their conclusions and vigorously criticizing the research methods on its blog and in a press call held on the same day the report was made public. Voatz called the research "flawed"[19] and "riddled with holes"[20] as its officers claimed the attacks MIT identified were impossible.[21]

Even though the DHS had validated MIT's findings, Voatz's strenuous denials and attacks on the MIT report were successful in convincing some of its customers that Voatz's security claims were valid and that the MIT findings were false. Utah County Clerk Amelia Powers Gardner repeated the same spurious explanations Voatz had provided to reporters when justifying the continued use of the application and told reporters there was no evidence the researchers' findings raised security concerns.[22] Jackson County Clerk Christine Walker told the press that Jackson was still planning on using Voatz's system for the 2020 primary.[23]

One of Voatz's most vocal supporters, West Virginia Secretary of State Mac Warner, defended Voatz also by repeating the same claims Voatz had made in its press call.[24] As Voatz was withstanding a barrage of media criticism about the MIT study, Warner went even further in his support of Voatz by providing to reporters what was described by his office as a recently declassified DHS report.[25] The purported DHS report was not a security review but a hunt assessment report – essentially an analysis to determine if Voatz's network contained any evidence that it had been breached. This report provided found no evidence of any breaches and

---

[19] https://blog.voatz.com/?p=1209
[20] https://blog.voatz.com/?p=1243
[21] *Ibid.*
[22] Connor Richards, "Utah County still plans on using voting app despite security concerns raised by researchers," *Daily Herald,* February 17, 2020. *Available at: https://www.heraldextra.com/news/local/govt-and-politics/utah-county-still-plans-on-using-voting-app-despite-security/article_ae0d1c54-8b17-5a09-9946-3f3585bda72f.html*
[23] Lydia Emmanoulidou, "MIT researchers sound alarm over voting app's security flaws," *Public Radio International,* February 14, 2020. *Available at: https://www.pri.org/stories/2020-02-14/mit-researchers-sound-alarm-over-voting-app-s-security-flaws*
[24] Steven Allen Adams, "Warner pushes back on claims of voting app vulnerabilities," *News and Sentinel,* February 15, 2020. *Available at: https://www.newsandsentinel.com/news/local-news/2020/02/warner-pushes-back-on-claims-of-voting-app-vulnerabilities/*
[25] Danny Nelson, Nikhilesh De, Ben Powers, "MIT Wasn't Only One Auditing Voatz-Homeland Security Did Too, With Fewer Concerns," *Coindesk,* February 14, 2020. *Available at: https://www.coindesk.com/mit-wasnt-only-one-auditing-voatz-homeland-security-did-too-with-fewer-concerns*

only minor security issues. It was distributed to reporters by the West Virginia Secretary of State and was reported in multiple news stories, serving as a counterweight to the damaging MIT study.[26]

Though the West Virginia Secretary of State's office described the report as a DHS report, and in several cases reported by the media to be a DHS study, it was, in fact, ***a report drafted and published by Voatz itself*** purporting to represent what the (still non-public) DHS hunt report found.[27]

Approximately a month after the MIT study was published, the independent security firm Trail of Bits (TOB) released a security review it conducted of the Voatz mobile voting platform on behalf of Tusk Philanthropies and Voatz. The Trail of Bits' study was a searing indictment of Voatz's security, affirming all of the assertions made by the MIT team and identifying additional security vulnerabilities in the system. Further, the Trail of Bits study exposes many of the public statements Voatz made in response to the MIT study as false, misleading or specious. According to the Trail of Bits report, TOB confirmed to Voatz all the security vulnerabilities identified by MIT on February 11th, *two days before* Voatz published its response to the MIT study and held a press call falsely denying the findings in the MIT report. We have excerpted some of these statements in Attachment A along with other statements from Voatz's website which—taken together with the Appendix to the MIT study—support our concerns that Voatz has been making false, misleading or deceptive claims to promote and sell its product.

III. Voatz's actions warrant revocation of its corporate charter.

Voatz's repeated false claims and misstatements about the security of its voting platform should be held to constitute "abuse" of its corporate charter. The interest of the public should be the primary consideration when considering whether to revoke a corporate charter. *See State v. Cortelle Corp.*, 38 N.Y.2d 83, 341 N.E.2d 223 (N.Y. 1975). Eliminating Voatz's corporate protections would best serve the public interest. Serious misrepresentations demand serious consequences, and Voatz has proved that it holds honesty and fair dealing in low regard. Furthermore,

---

[26] Anthony Kimery, "Voatz blockchain voting app security questioned in new study; DHS seems unconcerned," *Biometric Update,* February 17, 2020, *available at: https://www.biometricupdate.com/202002/voatz-blockchain-voting-app-security-questioned-in-new-study-dhs-seems-unconcerned*; Dave Mistisch, "MIT Study: Mobile Voting App Used in W.VA Pilot Susceptible To Hacks That Could Change Votes," *West Virginia Public Broadcasting,* February 13, 2020. *Available at: https://www.wvpublic.org/post/mit-study-mobile-voting-app-used-wva-pilot-susceptible-hacks-could-change-votes#stream/0.*

[27] https://voatz.com/Hunt-Engagement-Summary-Voatz.pdf

Voatz's conduct, in violation of multiple states' laws, should constitute "abuse" and lead to the revocation of its corporate charter. While the states in which Voatz operated will be able to exact punishment for the misdeeds committed within their borders, only Delaware has the power to ensure that Voatz is permanently disabled from fraudulently selling its platform as secure and uncorruptible.

By repeatedly declaring its voting system safe when it knew the system was insecure, Voatz engaged in a persistent course of fraudulent conduct warranting an investigation into its abuse of its corporate charter. Under the Delaware Constitution and revocation law, "the Court will forfeit a corporate charter where the abuse of its privileges and franchises is clear." *Young*, 109 A.2d at 29.

We respectfully urge you to investigate whether, as seems clear, Voatz has forfeited the privilege of its corporate charter, and to initiate forfeiture proceedings using your authority under Title 8.

Thank you very much for your consideration. Please do not hesitate to reach out to us if you have any questions or if we can be of any assistance.

Sincerely,

Susan Greenhalgh, Senior Advisory on Election Security
Ron Fein, Legal Director

Attachment A – Voatz's statements on security

1. Excerpt from the Trail of Bits report responding to Voatz criticism of the MIT study:

   "Objection 1
   The researchers were analyzing an Android version of the Voatz mobile voting app that was at least 27 versions old at the time of their disclosure and not used in an election.
   The version of the app assessed by the MIT researchers was from late September 2019, approximately four months before they started their assessment. In our review, we did not identify any security relevant changes in the codebase between September 2019 and the code delivered at the start of this engagement other than: 1) minor changes to Zimperium; and 2) a minor change in the cryptographic handshake protocol. Neither change substantively affects MIT's claims.

   Objection 3
   In the absence of trying to access the Voatz servers, the researchers fabricated an imagined version of the Voatz servers, hypothesized how they worked, and then made assumptions about the interactions between the system components that are simply false. This flawed approach invalidates any claims about their ability to compromise the overall system. In short, to make claims about a backend server without any evidence or connection to the server negates any degree of credibility on behalf of the researchers.

   Developing a mock server in instances where connecting to a production server might result in legal action is a standard practice in vulnerability research. It is also a standard practice in software testing. The MIT findings are focused within the Android client and do not rely on intimate knowledge of the Voatz servers."

2. Excerpts from Voatz' February 13, 2020 press call, also posted on Voatz blog.

   a. *…the next set of questions come from Russell Brandom from The Verge. First question is, I understand from the post that the MIT researchers were testing an outdated version of your software and weren't connected with Voatz servers. However, the post stops short of saying that the vulnerabilities discovered had been patched in recent version. I'm curious if you can speak directly to the status of those vulnerabilities.*

      Nimit Sawhney, Voatz CEO & Co-founder: *Absolutely. So they had whole paper is riddled with holes, if I can use that word. For example, they talk about our use of the blockchain and say, executing a 51 percent attack. That attack is not possible because we do not use a public blockchain. We use a*

permissioned blockchain based on Hyperledger, and such an attack is not possible on that infrastructure.

Fifty-one percent attacks cannot be taken against Hyperledger but this is irrelevant. Instead, Hyperledger can be taken over by compromising only a third of the network without any further action. In either case, both Azure and Amazon Web Services could easily take over the network.

Moreover, the MIT analysis explicitly assumes the blockchain is secure. The vulnerabilities found exist with other segments of the platform which make ballots susceptible to online manipulation, deletion or spying.

b. ***Sawhney****: Similarly, [MIT] assume that by defeating the malware and the jailbreak detection on the mobile devices, that they will be able to connect to our server. Because they didn't connect to our server, they did not experience all the checks which happen on the server, which would have prevented them from doing anything… And then all of their claims are based off that. That because they were able to jailbreak or successfully compromise a client device, that the assumption that device would be able to connect to our server is completely, completely flawed*.

The Trail of Bits report confirmed the MIT findings:

B.6 Server compromise
[MIT] Claim: The anonymous researchers who submitted the report to DHS speculate (but have no proof) that anyone with access to the API server can alter, expose, or discard any user's vote. They also observe that there is no evidence of any blockchain verification code in the client.
Status: Confirmed, on all accounts. However, in order to alter a vote that has already been cast, the attacker would also need to have control over the Hyperledger Fabric blockchain. The credentials for accessing the blockchain are stored on the API server. An attacker who can modify the software running in the API server can alter, expose, or discard any user's vote. The clients do not interact with the blockchain directly, so there is no blockchain verification code in the client.

c. ***Larry Moore, Senior Vice President:*** *Nimit, a reminder to talk about the first claim on the side channel link.*

Nimit Sawhney, CEO & Co-founder: *Yes, I was getting there. So one of the [MIT] claims they have is, as Larry mentioned, it's called a side channel leak. To drill it down, what it means is as network traffic is passing through while*

people are using their devices, that by looking at that encrypted network traffic, they can deduce who you are voting for, and then start disrupting that traffic to the disadvantage of the voter. And hypothetically, that may be possible. In a realistic scenario, that's not possible given how our pilots are conducted. Secondly, that issue of a side channel problem was fixed many months ago. So if they had used the newer version of our system, they wouldn't have even seen that. But we want to reiterate that in a real world scenario, exploiting that is extremely, extremely hard. Especially in the case of our pilots where voters are distributed, it's a smaller amount of voters. They're distributed around the world, breaking into network routers, cell towers, isolating individual voters, breaking into their devices… I mean, these are… This is hypothetical scenario. It's not realistic at all.

Trail of Bits confirmed MIT's findings:

B.1 Side-channel information leak

Claim: A passive observer can determine the ballot entries of a voter solely by the size of their encrypted vote submission message.
Status: Voatz claims that the clients have been modified to include padding before the ballot data is transmitted. However, we were unable to find this feature in the codebase. Padding does occur within the backend, however. It may be the case that it was added to clients in a feature branch that has not yet been merged into the development branch, and therefore was not provided to us.

B.2 Voter disenfranchisement via network disruption

Claim: An active network participant (*e.g.* , one with control over any node in the route from the voter to the Voatz API server) can choose to drop a user's messages to the Voatz server. Moreover, the mechanism described in B.1 can be exploited to selectively drop only ballots that contain certain votes.
Status: Confirmed. There is no mechanism that would prevent this attack.

B.3 On-device security circumvention

Claim: The libraries used for threat detection in the mobile clients can be disabled on rooted devices, allowing the clients to be run on unsupported devices as well as with modified versions of the client.
Status: Confirmed. We were able to build a version of the Android application with threat detection disabled. There does not appear to have been any additional mitigations added since version 1.1.60. See finding TOB-VOATZ-29 .

B.5 PIN cracking

Claim: An attacker with access to the Voatz app's storage (*e.g.* , on a rooted device) can trivially compromise a user's Voatz PIN, even if the Voatz app is not running.

Status: Confirmed. See TOB-VOATZ-048 .

3. **Claims taken from Voatz FAQ:**

   a. *Voatz claims that it maintains voter anonymity through the use of "mixnets."*

   How do I vote? Voting with Voatz is only available in elections that are engaging the technology on a pilot-basis or on a contractual-basis.

   If voting in an eligible election, the process begins when an eligible voter receives a ballot from their county, typically at the beginning of the early voting window. The voter will receive a red badge notification from their Voatz app, indicating they now have the option and eligibility to cast a ballot(s) in an ongoing election. The voter opens the Voatz app on his or her smartphone and unlocks it with their fingerprint or Face-ID to begin voting. Selections for choices (candidates or ballot questions) are made one contest at a time by touching a candidate's name. Voters are prevented from selecting more choices than allowed to ensure that only their allotted number of votes count. At any time before submission, the voter can review their choices and make changes if necessary. Once finished, the voter submits their ballot. Once submitted, all information is anonymized, routed via a "mixnet" and posted to the blockchain."

   The Trail of Bits report confirms that there is no evidence that mixnets are present in the Voatz code. Further it confirms that it's possible to deanonymize the ballots and compromise voter privacy.