April 20, 2020

The Honorable Phil Weiser
Office of the Attorney General
Colorado Department of Law
Ralph L. Carr Judicial Building
1300 Broadway, 10th Floor
Denver, CO 80203

Dear Attorney General Weiser,

We write to you to urge you to initiate an investigation into the voting system vendor Voatz for advancing potential false claims and deceptive marketing practices while promoting its mobile voting application in Colorado that may violate the Colorado Consumer Protection Act; Colo. Rev. Stat. §§ 6-1-101 *et seq*.; fraudulent misrepresentation; or any other violation of state law.[1]

Voatz is Boston-based startup company that is developing and aggressively marketing an internet-based voting system that enables voters to cast a ballot from application loaded on to their mobile phones. In 2019, the City of Denver contracted to have Voatz offer its internet voting system to voters eligible under the Uniformed and Overseas Citizen Absentee Voting Act (UOCAVA) for Denver's 2019 municipal elections. According to its contract with the City of Denver, Voatz (working with the National Cybersecurity Center and Tusk Philanthropies), declared that "it is their intention to advocate to the Office of the Secretary of State that the Solution be used statewide."[2]

Voatz's campaign to promote its voting system in the state of Colorado has included bogus claims of "military grade security,"[3] public statements asserting that votes cast on

---

[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] Agreement between City and County of Denver, Tusk Philanthropies, National Cybersecurity Center and Voatz," https://cse.sc.edu/~buell/blockchain-papers/documents/Contract_Tusk_Voatz_NCC_201948381_2019-03-18.pdf

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

its platform could not be deleted or altered,[4] and published materials[5] and presentations[6] promising that Voatz's system was robustly vetted and secure.[7] Though many computer security experts vociferously expressed skepticism or distrust at Voatz's claims as unsupported, spurious or misleading[8],[9] the City of Denver elected to engage Voatz to offer its mobile voting system for military and overseas voters in Denver's 2019 municipal elections.

In a press release issued by Voatz's sponsor, Tusk Philanthropies, Denver County 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." Bucaro's endorsement of Voatz indicates Voatz's campaign to persuade Colorado election officials that its system is secure was fruitful.

Though Voatz's unproven advertisements regarding security successfully persuaded election officials in Denver as well as Utah, West Virginia, and Oregon, Voatz's failure to substantiate any of these statements continued to breed 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."*[10]

---

[4] Robert Hackett, "Denver and West Virginia Deserve Praise for Voting on Blockchain," *Fortune,* March 23, 2019
https://fortune.com/2019/03/23/blockchain-vote-election-denver-west-virginia-voatz/
[5] https://blog.voatz.com/wp-content/uploads/2019/02/West-Virginia-Mobile-Voting-White-Paper-NASS-Submission.pdf
[6] Ibid.
[7] Voatz, "Frequently Asked Questions," https://www.voatz.com/faq.html
[8] Maya Kosoff, "A Horrifically Bad Idea: Smartphone Voting is Coming Just in Time for the Midterms," *Vanity Fair,* August 7, 2018
[9] Dr. David Jefferson, et al, "What We Don't Know About the Voatz "Blockchain" Internet Voting System," May 1, 2019, https://cse.sc.edu/~buell/blockchain-papers/documents/WhatWeDontKnowAbouttheVoatz_Blockchain_.pdf
[10] *Available at*: https://www.washingtonpost.com/context/sen-ron-wyden-d-ore-letter-regarding-voatz/e9e6dd4f-1752-4c46-8e37-08a0f21dd042/

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 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*."[11]

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."[12]

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.[13] This list provides a preliminary foundation to establish that Voatz's security claims are faulty.

---

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

[12] 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.

[13] *Ibid.*

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 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"[14] and "riddled with holes"[15] as its officers claimed the attacks MIT identified were impossible.[16]

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.[17] Denver County clerk/recorder Jocelyn Bucaro was less emphatic but remained supportive of Voatz, stating that the County was "very happy with [Voatz]."[18]

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.[19] 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

---

[14] https://blog.voatz.com/?p=1209
[15] https://blog.voatz.com/?p=1243
[16] *Ibid.*
[17] 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
[18] Matt Mauro, "MIT study: voting app that Denver used could be hacked," *KDVR Fox 31,* February 13, 2020. *Available at:* https://kdvr.com/news/politics/mit-study-voting-app-that-denver-used-could-be-hacked/
[19] 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/

office as a recently declassified DHS report.[20] 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 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.[21]

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.[22]

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.

We urge you to review this information and ask you to initiate an inquiry to determine if Voatz has engaged in or is engaging in any deceptive trade practices under the Colorado Consumer Protection Act, Colo. Rev. Stat. §§ 6-1-101 *et seq*.; fraudulent misrepresentation; or any other violation of state law.

---

[20] 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*

[21] 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.

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

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

Sincerely,

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

cc. The Honorable Jena Griswald
Colorado Secretary of State

Representative Jerrold Nadler
Chair, House Committee on the Judiciary
U.S. House of Representatives

Representative David Ciccilline
Chair, Subcommittee on Antitrust, Commercial and Administrative Law
House Committee on the Judiciary
U.S. House of Representatives

Representative Joe Neguse
Vice Chair, Subcommittee on Antitrust, Commercial and Administrative Law
House Committee on the Judiciary
U.S. House of Representatives