June 4, 2020

The Honorable Maura Healey
Office of the Attorney General
One Ashburton Place
Boston, MA 02108

Dear Attorney General Healey,

We write to urge you to initiate an investigation, pursuant to your authority under the Massachusetts Consumer Protection Act, G.L. c. 93A § 6, into the voting system vendor Voatz for participating in potentially false and deceptive marketing practices while promoting its mobile voting application to both consumers and investors from its headquarters in Boston, Massachusetts.[1]

Voatz is a Boston-based startup company that is developing, aggressively marketing, and soliciting investments in its internet-based voting system that enables voters to cast a ballot from an application loaded on to their mobile phones.[2] Computer and network security experts are virtually unanimous that online voting is an exceedingly dangerous threat to the integrity of U.S. public elections.[3] Nonetheless, Voatz's successful campaign to promote its online voting

[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] shorturl.at/gmxFN; The investors whom Voatz appears to have misled by its deceptive practices are based both in the commonwealth and in other states. *See* Voatz on Crunchbase, https://www.crunchbase.com/organization/voatz#section-investors (last visited May 29, 2020).

[3] David Jefferson, "If I Can Shop and Bank Online, Why Can't I Vote Online?," Verified Voting, https://www.verifiedvoting.org/resources/internet-voting/vote-online/ (last visited May 28, 2020).

system in public elections throughout the United States has included bogus claims of "military grade security."[4]

In February of this year, the public had its first look at Voatz's security from an independent third party when researchers at the Massachusetts Institute of Technology (MIT) published a report contradicting much of Voatz's claims of security. 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."[5]

In addition to documenting multiple, significant vulnerabilities with Voatz's 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.[6] This list provides a preliminary foundation to establish that Voatz's security claims are faulty.

Voatz responded to the MIT researchers' findings forcefully, staunchly denying their conclusions and vigorously criticizing the research methods both on its blog and in a press call held on the same day the report was made public. Voatz called the research "flawed"[7] and "riddled with holes"[8] as its officers claimed the attacks MIT identified were impossible.[9]

---

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

[5] 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.

[6] *Id.*

[7] https://blog.voatz.com/?p=1209

[8] https://blog.voatz.com/?p=1243

[9] *Id*.

These statements appear to have been made by Voatz staff from their office in Boston.[10] Indeed, according to its LinkedIn profile, Voatz has at least 20 employees located in the greater Boston area and thus likely conducts much of its marketing practices from Massachusetts.[11]

Voatz's unproven advertisements regarding security have successfully persuaded election officials in Denver, Utah, West Virginia, and Oregon to use its system, but Voatz's failure to substantiate any of these statements still 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."[12]

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*."[13]

---

[10] *Id*. ("[W]e're probably less than two miles away as the crow flies from the MIT Research Lab in Downtown Boston, so we're close. They could have contacted us. Had they invited us over, we had come over on the red line").

[11] Voatz LinkedIn, https://www.linkedin.com/company/voatz/ (last visited May 28, 2020).

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

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

The ShiftState report has still not been released.

After conducting their research, the MIT researchers had 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.

Although DHS had validated MIT's findings, Voatz's 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 provided reporters when justifying the continued use of the application, telling reporters there was no evidence researchers' findings raised security concerns.[14] Denver County clerk Jocelyn Bucaro was less emphatic but remained supportive of Voatz, stating that the County was "very happy with [Voatz]."[15]

One of Voatz's most vocal supporters, West Virginia Secretary of State Mac Warner, also defended Voatz by repeating the same claims Voatz made in its press call.[16] As Voatz endured a barrage of media criticism about the MIT study, Warner went even further in his support of Voatz by providing to reporters what his office

---

[14] 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

[15] 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/

[16] 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/

described as a recently declassified DHS report.[17] 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 it had been breached. This document reported 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.[18]

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.[19]

Approximately one 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.[20] The Trail of Bits' study was a searing indictment of Voatz's security, affirming all assertions made by the MIT team and even 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

---

[17] 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*

[18] 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.

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

[20] https://github.com/trailofbits/publications/blob/master/reviews/voatz-securityreview.pdf

specious. According to the report, on February 11, *two days before* Voatz published its response to the MIT study and held a press call falsely denying the findings in the MIT report, TOB had confirmed to Voatz all the security vulnerabilities identified by MIT. 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, from or at its headquarters in Massachusetts, through its marketing practices has engaged in or is engaging in any deceptive or unfair practices under chapter 93A, chapter 110A, or any other violation of state law.

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

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.