RITCHIE TORRES
15TH DISTRICT OF NEW YORK

1414 LONGWORTH HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-4361

Congress of the United States
House of Representatives
Washington, DC 20515-3215

February 12, 2024

Mr. Johnny Ayers
Chief Executive Officer
Socure
885 Tahoe Blvd, Street 11
Incline Village, Nevada, 89451

Dear Mr. Ayers:

In a digital age, proving one's identity online is essential for accessing critical services provided by government agencies, healthcare providers, and financial institutions. As the self-proclaimed "leading provider of digital identity verification" founded in New York, I am concerned about your company's practices, particularly as it relates to communities of color who face countless forms of digital discrimination.

The public is increasingly concerned about the role of data brokers and the behavior of companies that profit by purchasing, collecting, aggregating, licensing, selling, or sharing personal information. Americans are frequently upset to discover the abusive ways companies use their data, which is why Congressional leaders have raised questions to data brokers, including congressional hearings and letters questioning the practices of 22 companies.[1] As the representative for one of the most ethnically and socioeconomically diverse districts in the nation, I share my colleagues' concerns and want to ensure a company like Socure that is using personal data to broker access to critical services is held to a similar standard, particularly as the abuses of the data surveillance industry disproportionately harm people of color, low-income families, immigrants, LGBTQI+ individuals, and other vulnerable populations.[2]

You claim your product, "fuses personal identifiable information (PII) validated by thousands of data sources" in order to prevent fraud.[3] It is well-documented that systems built on large datasets can perpetuate inequality by offering lower quality of service for communities of color, whether that includes credit algorithms that are 5-10 percent less accurate for lower-income families and minority borrowers or sentencing software that overestimates the recidivism rates of

---

[1] House Energy and Commerce Committee, *E&C Leaders Continue Bipartisan Investigation into Data Brokers' Potential Exploitation of Americans' Privacy (May 10, 2023);* https://energycommerce.house.gov/posts/e-and-c-leaders-continue-bipartisan-investigation-into-data-brokers-potential-exploitation-of-americans-privacy.

[2] CFPB, *Protecting the Public from Data Brokers in the Surveillance Industry (August 15, 2023);* *https://files.consumerfinance.gov/f/documents/cfpb-data-broker-rulemaking-faq_2023-08.pdf*.

[3] Socure, *Socure Makes History as the World's First AI Technology to Successfully Solve for Account Opening Identity Fraud After 10+ Years of R&D (January 16, 2024);* https://www.socure.com/news-and-press/socure-solves-for-account-opening-identity-fraud.

Black women.[4] Companies' abuse of private data can also lead to the unwanted tracking and sale of people's sensitive health data, genetic information, religious participation, and location.[5] Given the lack of transparency around your services, constituents in my district have expressed legitimate privacy concerns and demand to know how you source their data, how it is used, and whether it is equitable for all American communities.

Your company's promotional materials describe your services being used by over 1,900 customers, including, "financial services, government, gaming, healthcare, telecom, and e-commerce industries, including four of the five top banks, the top credit bureau and more than 400 fintechs".[6] Such a broad use of your services, particularly for essential services including access to public sector agencies, justifies greater transparency and scrutiny around your practices to ensure you are properly serving all Americans, regardless of their background.

To assist in improving the understanding of Socure's practices related to the use of customer data, please respond to the following set of questions no later than 30 days from the date of this letter:

1. How do you test your fraud prediction models for bias, and do your models demonstrate any form of bias for communities regardless of race, gender, location, income, or sexual identity?

2. Socure publicizes that it has "thousands of data sources" – what are those data sources and how do they vary across user demographics?

3. How do you verify people who aren't in records, are unbanked, and don't participate in social media? Please provide the specific types of data you utilize to verify these individuals.

4. Do you purchase data on individuals from other data brokers or state agencies, like DMVs?

5. Does Socure scrape social media profiles as part of its data collection? If so, are users made aware? Do you retain social media data once a user deletes it from their account? How do you protect against fraudulent or fake information placed on social media about a real person?

---

[4] Stanford University Institute for Human-Centered Artificial Intelligence, *How Flawed Data Aggravates Inequality in Credit (August 6, 2021);* https://hai.stanford.edu/news/how-flawed-data-aggravates-inequality-credit. NPR, *Justice Department works to curb racial bias in deciding who's released from prison (April 19, 2022); https://www.npr.org/2022/04/19/1093538706/justice-department-works-to-curb-racial-bias-in-deciding-whos-released-from-pris*.

[5] FTC, *FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data (January 9, 2024); https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data*.

[6] Socure, *Socure Makes History as the World's First AI Technology to Successfully Solve for Account Opening Identity Fraud After 10+ Years of R&D (January 16, 2024);* https://www.socure.com/news-and-press/socure-solves-for-account-opening-identity-fraud.

6. Socure touts that it evaluates consumers' "IP geo-location" and "location history" – how does this work? Are these concentrated in low-income communities?

7. Socure also touts that it "excels in detecting unusual real-time user behavior patterns" – how does Socure track consumers' behavior in real time?

8. You mention analyzing operating systems and browser languages over multiple years. Are you tracking individuals' activity online? How? Do you know and record what websites people are visiting? If so, are they aware?

9. What behavioral data does Socure collect? From what sources? Is that data tested to mitigate bias across demographic groups?

10. Does Socure process any U.S. consumer data at its international offices? How does Socure mitigate the possibility that sensitive information on U.S. individuals could be exposed in a foreign country?

11. What does Socure's India office do? Is any component of their work focused on analyzing data of U.S. citizens? Is any of that data sensitive, and if so, what protections if any are in place to protect that data from being exposed in a foreign country?

12. Does Socure retain consumers' data after it verifies their identities? For how long?

13. Does Socure create and maintain files on individual consumers? If so, can consumers access their file or request their data be deleted?

14. Does Socure share or sell any U.S. consumer data (including PII) with third parties?

15. Socure touts its use of artificial intelligence and machine learning, even calling itself the leading provider of AI identity verification. How are your algorithms tested for risk of bias against individuals of color who face digital discrimination? Do you have human backstops to address any issues with the algorithms you utilize?

I look forward to your response.

Sincerely,

Ritchie Torres
Member of Congress