

## Fine Print Partners

<u>Team Member Name</u>	<u>Year</u>	<u>Major</u>
Dario Benes	Junior	Finance
Ashley Fearday	Junior	Finance & Economics
David Goodwin	Junior	Finance
Emalee Postma	Senior	Finance
Emma Takacs	Freshman	Accounting

**Advisor(s):** Taylor Daum

**Topic Title:** The Price of Access: Biometrics and Financial Inclusion

**Audience:** Access Now Board of Directors

### Sustainable Development Goal

SDG #10: Reduce inequality within and among countries.

SDG #16: Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels.

### Executive Summary

As 1.3 billion adults worldwide remain unbanked, FinTech companies are increasingly offering financial access in exchange for permanent biometric data. Economically vulnerable populations are being targeted under conditions that various courts have ruled nonconsensual. Our committee examines Worldcoin (now "World") as a case study. Its Orb device has scanned approximately 12 million irises, effectively exchanging users' permanent biometric identity for ~\$50. This pattern goes beyond one company. India's Aadhaar system has suffered data breaches exposing over 1 billion records. In West Africa, vulnerable populations risk losing access to essential services if they refuse Mastercard-backed platforms that combine personal health data and payment systems. This issue sits at the center of the Sustainable Development Goals. SDG 16 calls for legal identity for all and the protection of fundamental freedoms like privacy, while SDG 10 seeks to reduce inequality. Biometric financial inclusion efforts are meant to advance these goals, but when poorly regulated, they place the greatest risks on the poorest communities while the profits and data flow to powerful global corporations.

Access Now has already flagged the risks of biometric digital identity systems through its #WhyID campaign, but these protections remain largely voluntary. Access Now should expand this work by pushing regulators to make its digital identity standards mandatory across the industry. These standards include strict limits on data retention, on-device processing, and transparency about how biometric data is collected and used. Privacy-protecting technologies such as zero-knowledge proofs, self-sovereign identity, and cancelable biometrics already show that financial inclusion can be built without storing unnecessary biometric data. The real issue is not technological limits, but business choices that prioritize data extraction over user protection.