# Use Cases and Capabilities

Current status and open questions

# **Background** Anti-Fraud Use Cases

Earlier this year, the working group collaborated on a document covering fraud patterns and use cases for consideration in this forum:

https://github.com/antifraudcg/use-cases/blob/main/USE-CASES.md

We subsequently agreed to add a ‘Capabilities’ section, where we would list key technologies for fraud mitigation. Proposals were streamlined into a single pull request:

https://github.com/antifraudcg/use-cases/pull/5

There are open comments on the PR, and there does not appear to be consensus in terms of how these should be articulated. We should align on an approach.

# Some examples that inspired some back and forth

"### Recognize whether the same device is seen again in the context of multiple identities"

*"There are legitimate cases of device sharing, which we will have to navigate. Would it be reasonable to express this as "Recognize whether an inordinate number of identities share the same device"? What "inordinate" means may vary across contexts, but we should be mindful of access through libraries and other shared resources ... Could a bucketed count suffice?"*

#### Retrieve a device's IP address

*"Would it be possible to tease these apart a bit? IP address is one signal that's potentially giving us these capabilities:*

- *Build and maintain a reputation of networks connecting to your system (datacenters, geo-hopping proxies) (from VPN/TOR detection)*
- *Distinguish client endpoints for rate limiting (from IP for account creation)*
- *Distinguish client endpoints for resource binding (from IP for account takeover)*
- *Distinguish client endpoints for blocking / preventing repeat abuse*
- *Approximate geo location"*

#### Know the geographic location of the device

#### Know that the geographic location of a device is being manipulated

*"Could we combine these two as ";onfirm the geographic location of the device?'"*

# IP Address raises some questions…

Obscuring browser IP address would have widely felt consequences across various platforms.

Removing access would impact virtually every major security or fraud application.

Can we instead replace it with alternative capabilities?

Discussion:

https://github.com/antifraudcg/use-cases/pull/5#discussion_r961849330

# What is the appropriate level of abstraction for accepted capabilities?

-There is a tension between the availability of data to support current fraud mitigation practices vs abstractions that hide raw identifiers but provide a better privacy posture

-In all likelihood, the loss of existing data points will not coincide with a smooth transition to alternative approaches. This has potentially brutal consequences for fraud in areas like eCommerce, financial services, and the public sector.

-On a practical level, can we really build our way out of this situation? Is it realistic to think that we can anticipate and design for all of our needs, when the current practice in fraud mitigation is to rapidly adapt to changing circumstances using a range of strategies that may no longer be supported?

**What is our ultimate goal with respect to capabilities - do we enumerate existing practices or imagine new ones? Where do we draw the line?**

# Discussion