Q1.
Goal of this survey:

- **Ensure completeness of capabilities inventory**
- **Prioritize capabilities needed by the anti-fraud ecosystem**

Anonymity of information:

- **Only company region, industry, and size (number of employees) will be collected**
- **Company name is optional and may be filled out if you would like to be contacted for follow-up conversations**
- **Consolidated results (not individual responses) will be shared within W3C's Anti-Fraud Community Group**

Capabilities Gathering: Key terms to know

- **Capabilities: Capabilities are the high-level functional requirements for a given set of anti-fraud use cases, and are not specific to any sources of truth or technologies. Capabilities are aligned to specific use cases. For capabilities, please focus on capabilities that a browser can communicate about a device**

Q53. Where did you get a link to this survey?

○ 1:1 engagement with Google stakeholders

● Anti-Fraud CG Github

Q2. Would you like to have your individual response published publicly in W3C's Anti-Fraud Community Group with your company name visible? If yes, please add your company name below.

Note that consolidated results will be shared within the Anti-Fraud Community Group.

○ I do not want this individual response and company name published

● I want to publish this response individually with the company name F5

Q37. Would you like Google to reach out to you 1:1 to discuss these responses further? If yes, please include your name, email address, and company name below

Name	Michael Ficarra
Email Address	
Company Name	F5

Q3. Company Operating Region (select all that apply)

☑ North America

☐ South America

☑ Asia

☑ Europe

☐ Africa

☐ N/A - not representing an organization

Q4. Company Industry (select all that apply)

☑ Anti-Fraud Technology Providers

☐ eCommerce

☐ Financial Services (Banking, Payments, Cryptocurrency etc.)

☐ Social Media

☐ Content (Publishers, Streaming Services, Gaming etc.)

☐ Other

☐ N/A - not representing an organization

Q5. Company Size (number of employees)

○ 1-50

○ 51-500

● 501-10,000

○ 10,001-50,000

○ 50,001+

○ N/A - not representing an organization

Q7. To learn more about use cases, visit https://github.com/antifraudcg/use-cases/blob/main/USE-CASES.md

Q6. Which use cases are applicable to your organization? (select all that apply)

☑ Account Creation

☑ Account Takeover

☐ Invalid Traffic (IVT) in Advertising

☑ eCommerce Fraud

☑ Payment Fraud

☑ Data Scraping

☑ Online Spam & Fake Engagements

☑ Denial of Service

□ Theft of Intellectual Property

☑ Unauthorized Access

□ Other

□ Other

□ Other

Q9. Rank the use cases in order of importance (drag choices to move)

Account Takeover	1
Unauthorized Access	2
Payment Fraud	3
eCommerce Fraud	4
Account Creation	5
Data Scraping	6
Online Spam & Fake Engagements	7
Denial of Service	8

Q36. To learn more about capabilities visit https://github.com/antifraudcg/use-cases/issues/3

Q11. For the 'Account Creation' use case, select all relevant capabilities and add ones not listed below

☑ Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device

☑ Counters: Ability to keep an approximate count of how often a physical device has done a specific action

☑ Geo Attestation: Confirm the geographic location of a specific device

☑ Device and Boot attestation: Confirm that the device and OS matches the reported model and version

☑ User Presence: Confirm that a user is present

☑ Post-boot attestation: Check for up-to-date security patches and known strains of malware

□ Intent: Reason about the degree of coordination among an arbitrary set of users

□ App/Site attestation: Confirm that the application or website on the device matches the application or website reported to the service

□ Element Visibility: Confirm that a given visual element actually activated pixels on the device

☑ Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over

☑ Other a way to technologically enforce a "1 per person" limit

□ Other

□ Other

Q38. For the 'Account Creation' use case, rank all the relevant capabilities in order of importance

a way to technologically enforce a "1 per person" limit	1
User Presence: Confirm that a user is present	2
Counters: Ability to keep an approximate count of how often a physical device has done a specific action	3
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	4
Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over	5
Geo Attestation: Confirm the geographic location of a specific device	6
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	7
Post-boot attestation: Check for up-to-date security patches and known strains of malware	8

Q22. For the 'Account Takeover' use case, select all relevant capabilities and add ones not listed below

☑ Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device

☑ Counters: Ability to keep an approximate count of how often a physical device has done a specific action.

☑ Geo Attestation: Confirm the geographic location of a specific device

☑ Device and Boot attestation: Confirm that the device and OS matches the reported model and version

☑ User Presence: Confirm that a user is present

☑ Post-boot attestation: Check for up-to-date security patches and known strains of malware

☑ Intent: Reason about the degree of coordination among an arbitrary set of users

□ App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service

□ Element Visibility: Confirm that a given visual element actually activated pixels on the device

☑ Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over

☑ Other a way to technologically enforce a "1 per person" limit

□ Other

□ Other

Q39. For the 'Account Takeover' use case, rank all the relevant capabilities in order of importance

a way to technologically enforce a "1 per person" limit	1
User Presence: Confirm that a user is present	2
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	3

Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over	4
Intent: Reason about the degree of coordination among an arbitrary set of users	5
Geo Attestation: Confirm the geographic location of a specific device	6
Counters: Ability to keep an approximate count of how often a physical device has done a specific action.	7
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	8
Post-boot attestation: Check for up-to-date security patches and known strains of malware	9

Q21. For the 'Invalid Traffic (IVT) in Advertising' use case, select all relevant capabilities and add ones not listed below

This question was not displayed to the respondent.

Q40. For the 'Invalid Traffic (IVT) in Advertising' use case, rank all the relevant capabilities in order of importance

This question was not displayed to the respondent.

Q23. For the 'eCommerce Fraud' use case, select all relevant capabilities that can address the use case and add ones not listed below

☑ Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device

☑ Counters: Ability to keep an approximate count of how often a physical device has done a specific action

☑ Geo Attestation: Confirm the geographic location of a specific device

☑ Device and Boot attestation: Confirm that the device and OS matches the reported model and version

☑ User Presence: Confirm that a user is present

☑ Post-boot attestation: Check for up-to-date security patches and known strains of malware

☑ Intent: Reason about the degree of coordination among an arbitrary set of users

☐ App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service

☐ Element Visibility: Confirm that a given visual element actually activated pixels on the device

☑ Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over

☑ Other a way to technologically enforce a "1 per person" limit

☐ Other

☐ Other

Q41. For the 'eCommerce Fraud' use case, rank all the relevant capabilities in order of importance

a way to technologically enforce a "1 per person" limit	1

Counters: Ability to keep an approximate count of how often a physical device has done a specific action	2
Intent: Reason about the degree of coordination among an arbitrary set of users	3
User Presence: Confirm that a user is present	4
Geo Attestation: Confirm the geographic location of a specific device	5
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	6
Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over	7
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	8
Post-boot attestation: Check for up-to-date security patches and known strains of malware	9

Q24. For the 'Payment Fraud' use case, select all relevant capabilities that can address the use case and add ones not listed below

☑ Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device

☑ Counters: Ability to keep an approximate count of how often a physical device has done a specific action

☑ Geo Attestation: Confirm the geographic location of a specific device

☑ Device and Boot attestation: Confirm that the device and OS matches the reported model and version

☑ User Presence: Confirm that a user is present

☑ Post-boot attestation: Check for up-to-date security patches and known strains of malware

☑ Intent: Reason about the degree of coordination among an arbitrary set of users

□ App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service

□ Element Visibility: Confirm that a given visual element actually activated pixels on the device

☑ Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over

☑ Other a way to technologically enforce a "1 per person" limit

□ Other

□ Other

Q42. For the 'Payment Fraud' use case, rank all the relevant capabilities in order of importance

a way to technologically enforce a "1 per person" limit	1
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	2
Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over	3
Counters: Ability to keep an approximate count of how often a physical device has done a specific action	4
Intent: Reason about the degree of coordination among an arbitrary set of users	5

Geo Attestation: Confirm the geographic location of a specific device	6
User Presence: Confirm that a user is present	7
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	8
Post-boot attestation: Check for up-to-date security patches and known strains of malware	9

Q25. For the 'Data Scraping' use case, select all relevant capabilities that can address the use case and add ones not listed below

☑ Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device

☑ Counters: Ability to keep an approximate count of how often a physical device has done a specific action

☐ Geo Attestation: Confirm the geographic location of a specific device

☑ Device and Boot attestation: Confirm that the device and OS matches the reported model and version

☑ User Presence: Confirm that a user is present

☑ Post-boot attestation: Check for up-to-date security patches and known strains of malware

☑ Intent: Reason about the degree of coordination among an arbitrary set of users

☐ App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service

☐ Element Visibility: Confirm that a given visual element actually activated pixels on the device

☑ Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over

☐ Other

☐ Other

☐ Other

Q43. For the 'Data Scraping' use case, rank all the relevant capabilities in order of importance

Counters: Ability to keep an approximate count of how often a physical device has done a specific action	1
User Presence: Confirm that a user is present	2
Intent: Reason about the degree of coordination among an arbitrary set of users	3
Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	4
Recognize whether the same device is seen again in the context of multiple identities: For example, seeing many different identities' data coming from the same device can be indicative of account take over	5
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	6
Post-boot attestation: Check for up-to-date security patches and known strains of malware	7

Q26. For the 'Online Spam & Fake Engagement' use case, select all relevant capabilities that can address the use case and add ones not listed below

□ Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device

□ Counters: Ability to keep an approximate count of how often a physical device has done a specific action.

□ Geo Attestation: Confirm the geographic location of a specific device

□ Device and Boot attestation: Confirm that the device and OS matches the reported model and version

□ User Presence: Confirm that a user is present

□ Post-boot attestation: Check for up-to-date security patches and known strains of malware

□ Intent: Reason about the degree of coordination among an arbitrary set of users

□ App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service

□ Element Visibility: Confirm that a given visual element actually activated pixels on the device

□ Recognize whether the same device is seen again in the context of multiple identities (e.g., Seeing many different identities' data coming from the same device can be indicative of account take over)

□ Other

□ Other

□ Other

Q44. For the 'Online Spam & Fake Engagement' use case, rank all the relevant capabilities in order of importance

Q27. For the 'Denial of Service' use case, select all relevant capabilities that can address the use case and add ones not listed below

□ Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device

☑ Counters: Ability to keep an approximate count of how often a physical device has done a specific action.

☑ Geo Attestation: Confirm the geographic location of a specific device

☑ Device and Boot attestation: Confirm that the device and OS matches the reported model and version

☑ User Presence: Confirm that a user is present

☑ Post-boot attestation: Check for up-to-date security patches and known strains of malware

☑ Intent: Reason about the degree of coordination among an arbitrary set of users

□ App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service

□ Element Visibility: Confirm that a given visual element actually activated pixels on the device

□ Recognize whether the same device is seen again in the context of multiple identities (e.g., Seeing many different identities' data coming from the same device can be indicative of account take over)

□ Other

□ Other

□ Other

Q45. For the 'Denial of Service' use case, rank all relevant capabilities in order of importance

Counters: Ability to keep an approximate count of how often a physical device has done a specific action. 1

User Presence: Confirm that a user is present	2
Intent: Reason about the degree of coordination among an arbitrary set of users	3
Geo Attestation: Confirm the geographic location of a specific device	4
Device and Boot attestation: Confirm that the device and OS matches the reported model and version	5
Post-boot attestation: Check for up-to-date security patches and known strains of malware	6

Q28. For the 'Theft of Intellectual Property' use case, select all relevant capabilities that can address the use case and add ones not listed below

This question was not displayed to the respondent.

Q46. For the 'Theft of Intellectual Property' use case, rank all relevant capabilities in order of importance

This question was not displayed to the respondent.

Q29. For the 'Unauthorized Access' use case, select all relevant capabilities that can address the use case and add ones not listed below

☑ Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device

□ Counters: Ability to keep an approximate count of how often a physical device has done a specific action.

☑ Geo Attestation: Confirm the geographic location of a specific device

□ Device and Boot attestation: Confirm that the device and OS matches the reported model and version

□ User Presence: Confirm that a user is present

□ Post-boot attestation: Check for up-to-date security patches and known strains of malware

☑ Intent: Reason about the degree of coordination among an arbitrary set of users

□ App/Site attestation: Confirm that the application or website on the device match the application or website reported to the service

□ Element Visibility: Confirm that a given visual element actually activated pixels on the device

□ Recognize whether the same device is seen again in the context of multiple identities (e.g., Seeing many different identities' data coming from the same device can be indicative of account take over)

□ Other

□ Other

□ Other

Q47. For the 'Unauthorized Access' use case, rank all relevant capabilities in order of importance

Token Binding: With user consent, bind a credential (such as a cookie) to a specific physical device	1
Intent: Reason about the degree of coordination among an arbitrary set of users	2
Geo Attestation: Confirm the geographic location of a specific device	3

Q30. For the '' use case, select all relevant capabilities that can address the use case and add ones not listed below

This question was not displayed to the respondent.

Q48. For the '' use case, rank all relevant capabilities in order of importance

This question was not displayed to the respondent.

Q31. For the '' use case, select all relevant capabilities that can address the use case and add ones not listed below

This question was not displayed to the respondent.

Q49. For the '' use case, rank all relevant capabilities in order of importance

This question was not displayed to the respondent.

Q32. For the '' use case, rank all relevant capabilities in order of importance

This question was not displayed to the respondent.

Q50. For the '' use case, rank all relevant capabilities in order of importance

This question was not displayed to the respondent.

Q35. If an out-of-band feedback mechanism existed, would you be willing to provide the attestet with feedback (e.g. via RPC) on attestations associated with abuse of your services?

● Yes

○ No

Q34. Please share any other feedback and questions below