

Privacy Threshold Overview (SKAN 4.0)

Built for you by Dataseat – contextual privacy-focused mobile DSP

With SKAN Apple introduced privacy thresholds to ensure postbacks sent to the advertiser / ad-network could not be tied back to an individual user. Apple will withhold important postback information (parameters) if privacy thresholds (i.e., install volume by campaign within a 24-hour period) are not met. You will find the list of the postback parameters subject to privacy thresholds below.

SKAN 4.0 Postback parameters subject to privacy thresholds

✓ **Source ID (formerly campaign ID):**

The unique identifier assigned to a SKAN campaign. This is returned back in the form of a two-, three-, or four-digit number, depending on the level of privacy threshold met. Source ID is assigned by the ad network/DSP.

✓ **Source app ID (applicable to app traffic only):**

The **Apple app ID** where the install came from (i.e., where the winning ad appeared).

✓ **Source domain (applicable to web traffic only):**

The **website domain** where the install came from (Safari browser only).

✓ **Conversion value (coarse-grained):**

General insights into the in-app actions a user takes post-install. This is returned back as **high, medium, or low**, in advertiser-defined groupings. Coarse-grained conversion values are subject to **lower privacy thresholds** than fine-grained and can be received during the **first, second, and third postback windows**.

✓ **Conversion value (fine-grained):**

Detailed insights into the in-app actions a user takes post-install. This is returned back in the form of a **number (0-64)** assigned by the advertiser. Fine-grained conversion values are subject to a **higher privacy threshold** than coarse-grained and can only be received during the **first postback window**.

Summary of postback windows

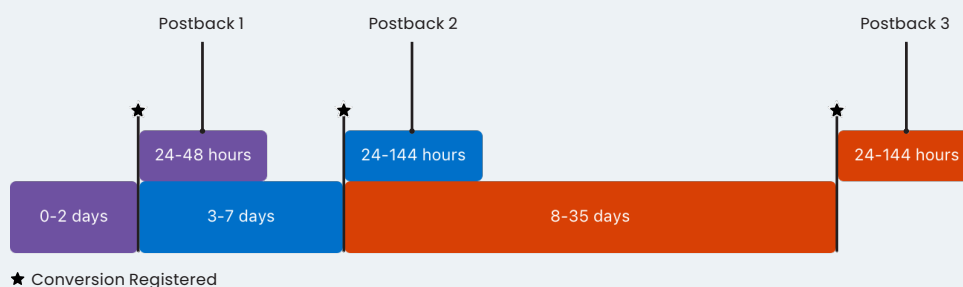
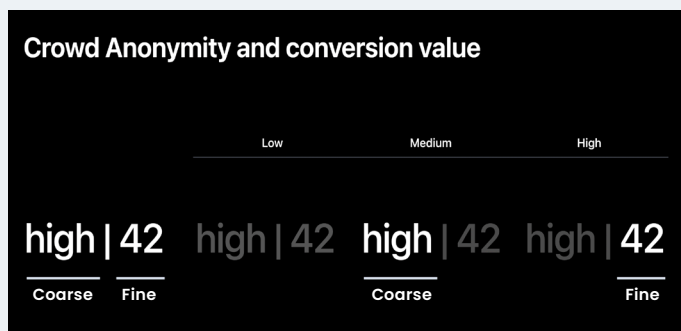


Image source: [Apple](#)

Conversion value example



Source identifier example

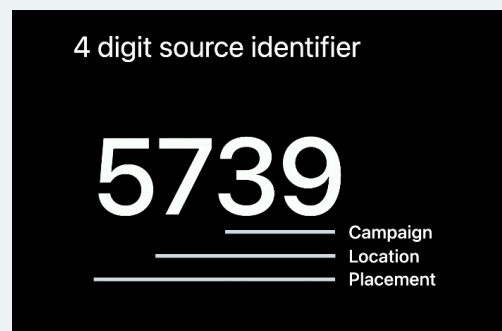


Image source: [Apple](#)

Summary of crowd anonymity tiers:

With SKAN 4.0, Apple brought forth the concept of crowd anonymity to allow for more actionable campaign data to be returned to the advertiser / ad-network while maintaining user privacy. There are now four tiers of crowd anonymity (while previous versions of SKAN only had one tier) which are determined by Apple and based on install volume by campaign (crowd size). The crowd anonymity tiers and associated postback parameters returned are as follows:

Tier 3 - Highest crowd anonymity data received:

- ✓ Fined-grained conversion value
- ✓ Source App ID
- ✓ 4-digit Source ID

Tier 2 - High crowd anonymity data received:

- ✓ Fine-grained conversion value
- ✓ 4-digit Source ID

Tier 1 - Medium crowd anonymity data received:


- ✓ Coarse-grained conversion value
- ✓ 2-digit Source ID

Tier 0 - Low crowd anonymity data received:

- ✓ 2-digit Source ID

To book a call with one of our experts or discuss your SKAN setup and potentially running UA campaigns on Dataseat, reach out to us.



Now part of  VERVE GROUP

Contextual privacy-focused mobile DSP

One of our ongoing goals is to improve measurability of mobile UA campaigns using iOS SKAdNetwork, and we pride ourselves on being the industry's longest standing experts in SKAN. We navigate within the constraints of crowd anonymity and privacy thresholds and enable our advertisers with solutions that make their SKAN-only campaigns optimizable and more efficient.

www.dataseat.com