

# EXHIBIT 1

***REDACTED VERSION OF DOCUMENT  
SOUGHT TO BE SEALED***

## **EXHIBIT 1 – FACEBOOK’S SECURITY COMMITMENTS**

Pursuant to the Parties’ Settlement Agreement, filed concurrently in the matter captioned *Adkins, et al. v. Facebook, Inc.*, Case No. C 18-05982 WHA (JSC), Facebook shall adopt, implement, and/or maintain the security commitments as described below, for a period of five years from the Effective Date of the Parties’ Settlement Agreement.

1. Facebook shall utilize tools reasonably designed to run integrity checks<sup>1</sup> on session updates (*i.e.*, significant changes [REDACTED], [REDACTED] during the course of a session).<sup>2</sup> Specifically, these tools shall be reasonably designed to run integrity checks on:
  - (a) [REDACTED]; and
  - (b) [REDACTED]
2. Facebook shall utilize tools reasonably designed to detect suspicious patterns in the generation and use of access tokens across Facebook. Specifically:
  - (a) Facebook shall utilize monitoring rules reasonably designed to detect [REDACTED]<sup>3</sup> [REDACTED] tokens issued or received by Facebook<sup>4</sup>; and
  - (b) Facebook shall implement alerting rules, processes, and procedures reasonably designed to automatically bring such changes to the attention of appropriate security personnel.
3. Facebook shall utilize processes, procedures, and tools reasonably designed to enable Facebook to promptly contain a security incident involving the improper issuance of access tokens. Specifically, Facebook shall utilize tools that enable

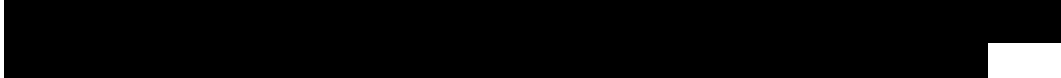
---

<sup>1</sup> An “integrity check” refers to an automated assessment of user activity for signals of theft or abuse of user credentials, based on a comparison of various parameters of the user’s current session against the user’s login history.

<sup>2</sup> A “session” refers to the set of user activity starting from a login to a Facebook product from a particular device or application. For example, a user who logs into Facebook from a browser on a desktop computer, from the Facebook mobile app, and from a browser on a mobile device would have three separate sessions corresponding to the activity following from these three logins.

<sup>3</sup> The term “specified” as used in this document means selected by the Facebook team responsible for the security measure at issue.

<sup>4</sup> “Issuance” of a token refers to the transmission of a token by Facebook to a user. “Receipt” of a token refers to the transmission of a token from an application to Facebook on a user’s behalf in connection with accessing the user’s account.

- 
4. Facebook shall utilize systems reasonably designed to generate automatic alerts for specified types of suspicious activity observable in user growth metrics. Facebook shall also utilize automated processes reasonably designed to ensure that a site-event report (“SEV”) is filed if the alert is not promptly resolved and that the SEV is promptly addressed.
  5. Facebook shall obtain annual SOC2 Type II security assessments of certain Facebook products that cover the product security and vulnerability management controls used across Facebook’s infrastructure (including the Facebook service), and that apply the AICPA Trust Services Criteria for Security, Availability and Confidentiality.<sup>5</sup> The results of these annual SOC2 Type II security assessments shall be reported to the third-party vendor addressed in § 2.3 of the Settlement Agreement.
  6. Facebook shall utilize processes reasonably designed to implement the principle of least privilege so that applications that rely on access tokens are given only the capabilities needed to perform the functionalities for which they are intended. Specifically:
    - (a) Facebook shall maintain internal documentation that provides guidance to Facebook software engineers on best practices for selecting capabilities for applications that rely on access tokens.
    - (b) Facebook shall automatically remove any capabilities from a given application that relies on access tokens if the application does not use those capabilities over a 90-day period.
  7. Facebook shall certify that it has eliminated the use of “NoConfidence” authentication proofs<sup>6</sup> across the code for the Facebook service, and it shall not reintroduce the use of such authentication proofs in the code.
  8. Facebook shall commit to employing at least one senior security executive with direct reporting authority and obligations to Facebook’s Board of Directors.

---

<sup>5</sup> For the avoidance of doubt, a SOC2 assessment of a Facebook product other than the Facebook service may meet this requirement so long as it covers the product security and vulnerability management controls that apply to the Facebook service as well as the product that is the subject of the assessment.

<sup>6</sup> A “NoConfidence authentication proof” refers to a certain (now deprecated) interface in Facebook’s authentication infrastructure that was designed to enable a Facebook feature to generate a user credential without providing cryptographic proof of a valid login.

9. Facebook shall log issuance and receipt of access tokens across Facebook in a manner reasonably designed to facilitate the detection, investigation, and identification of the compromise of user access tokens. Specifically:
- (a) Facebook shall log access token issuance metadata [REDACTED] and reception metadata [REDACTED].
  - (b) Facebook shall retain the issuance metadata logs for [REDACTED] and the reception metadata logs for [REDACTED], subject to reasonable adjustment based on resource constraints.
  - (c) Facebook shall include in the logged [REDACTED], wherever such information is available.