Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

June 5, 2026

INCIDENT NOTIFICATION

Dear Attorney General Aaron Frey,

We are writing to inform you that a vulnerability in an Instagram account recovery support tool was used to potentially compromise the Instagram accounts of 30 users in your jurisdiction. All accounts have been secured to prevent any continued unauthorized access.

What Happened?

On May 31, 2026, Meta discovered that there was a vulnerability in an AI-assisted account recovery system for Instagram ("High Touch Support" or "HTS") that was exploited by unauthorized third parties to perform password resets on Instagram user accounts.

HTS is an AI-assisted support tool designed to help users who are locked out of their Instagram accounts regain access. Users can request support from HTS and, as part of that process, can ask that a password reset link be sent to their email address. The tool itself worked properly and functioned as intended; however due to a bug in a separate code path, the system did not properly verify that the email address provided by the individual requesting a password reset matched the email address associated with that user's Instagram account. As a result, when an individual provided an email address not previously associated with the account, the system incorrectly sent a password reset link to that unassociated email rather than rejecting the request. This allowed unauthorized third parties to receive a password reset link for accounts they did not own. Upon resetting the password, the unauthorized party was able to log in to the account if the account holder had not enabled two-factor authentication (2FA).

Categories of Personal Data Involved

We are unaware of what, if any, personal information was accessed; however, the following categories of personal information were potentially accessible within the Instagram accounts:

- Contact information (email address and/or phone number)
- Date of birth
- Social media posts and content (photos, videos, stories)
- Direct messages and communications
- Account activity and interaction history
- Profile information (biography, profile photo)
- Connected accounts and linked services

Potentially Impacted Users

30 users in Maine were potentially impacted, which includes users who had their passwords reset through the support tool, did not have 2FA enabled on their account and whose Instagram accounts were likely accessed by an unauthorized party. This number represents an upper bound of the users impacted as some of the accounts may have been accessed legitimately by account owners.

Measures Taken To Address the Incident

Upon discovery of the vulnerability, Meta took immediate steps to contain the incident and remediate affected accounts.

Immediate mitigation:

The same day the exploitation was identified by Meta, the following actions were taken to eliminate the attack vector:

- Disabled the AI-assisted support tool removing the vulnerable code path from production; and
- Invalidated all existing password reset links that had been generated through the vulnerable path, rendering any outstanding links generated by an unauthorized third party unusable.

Account remediation:

To secure accounts that may have been compromised and restore control to legitimate account owners, Meta undertook the following measures:

- Enrolled all potentially affected accounts into a mandatory security checkpoint requiring authentication before any account access, preventing any continued unauthorized access to users' accounts; and
- Instructed impacted users to reset their passwords and re-authenticate through secure, verified channels.

Longer-term measures:

Prior to re-launching the tool, Meta will fix the authentication check in the Instagram recovery entry point to ensure proper verification of email addresses against existing account information before any password reset is initiated. Additionally, Meta is conducting a comprehensive review of similar account recovery flows across Meta's platforms to identify and remediate any potential issues.

User Notifications:

As soon as practical, Meta intends to send user notifications to the potentially impacted users to inform them of this incident, recommend that they review their account security settings, and enable 2FA.

Sincerely,

Amber Hannah
Associate General Counsel | Incident Response Legal
Meta