Mobile Commons, LLC
32 Court St. Suite 904
Brooklyn NY 11201

Security Incident Report

11/10/25 Security Incident

Mobile Commons, LLC

Overview

On the evening of Monday, November 10th, an unauthorized third party gained illegal access to the mCommons platform through an account takeover, believed to be a spear phishing attack or similar social engineering method.

The intruder's access was active for a four-hour period ending at 12:10 AM on November 11th before being detected and access removed. A second access attempt was detected at 4:00 PM on November 13th and was immediately shut down. During these incidents, multiple attempts were made to send spam messages through the system. A limited number of these messages reached subscribers before existing security protocols identified and shut down the malicious activity.

No customer or subscriber personal data was compromised or accessed.

The team moved immediately to:

- Remove the intruder's access
- Contain any further attempted activity
- Assess the full scope of impact
- Notify affected customers
- Non-affected customers were notified via general communication

Current efforts involve working directly with mobile carriers, aggregators, and affected customers to strengthen the platform's security protocols and prevent similar attacks in the future. Messaging functionality has been suspended until there is confidence that the platform is secure.

Timeline

Monday, November 10, 2025

- 7:17-7:29 PM: Malicious broadcast activity detected through compromised inactive legacy customer accounts
- 9:00 PM: Suspicious activity flagged, incident response initiated
- 9:56 PM: Internal account with elevated privileges compromised, allowing unauthorized spam via customer short codes

Immediate Response:

- Disabled compromised accounts
- Invalidated and reset user passwords platform-wide
- Forced platform-wide session termination

- Mandatory password resets for administrative users

Tuesday, November 11, 2025

- Initial containment measures completed

Wednesday, November 12, 2025

- Deployed MFA enforcement for all mCommons admin users.

Thursday, November 13, 2025

- Second access attempt detected, and multiple attempts were made to send spam messages through the system
- A limited number of these messages reached subscribers before existing security protocols shut down the malicious activity
- Decision to pause all outbound messaging is made until added security measures are deployed (see Security Remediation)

Friday, November 14, 2025

- MFA is enabled for all internal MS365 users

Saturday, November 16, 2025

- Teams continued deploying items on the security roadmap (see below in Security Remediation)

Sunday, November 17-23, 2025

- No further suspicious activity detected since November 13
- MFA deployed on all mCommons and Hipcricket accounts

Root Cause

The incident originated when a member of our team downloaded a malicious file with imbedded credential harvesting software. The attacker gained access to accounts with elevated privileges that allowed access, enabling them to send messages through a limited number of short codes.

No customer or subscriber personal data was compromised or accessed.

Security Remediation

Below is a list of actions taken by Mobile Commons to mitigate the issue and future state in progress/planning:

Live Now:

Platform & Customer Security:

- All passwords reset - Nov 10-17, 2025
- Moved away from UCM authentication - Nov 10-17, 2025
- Minimum 60-minute advanced scheduling requirement - Nov 10-17, 2025 (manual screening)
- Monitoring of all access logs across platforms - Nov 10-17, 2025
- MFA deployed on all mCommons and Hipcricket accounts (email-based) - Nov 16, 2025

Internal & Corporate Security:

- MDM platform purchased & pilot launched - Nov 17, 2025
- Corporate MFA deployment - Nov 22, 2025
- KnowBe4 purchased (training and awareness) - Nov 19, 2025
- EDR plan developed - Nov 20, 2025
- Corporate mandatory Security and Awareness training – Dec 1, 2025
- OKTA meeting scheduled - Nov 21, 2025

Future State:

Platform & Customer Security:

- Platform SSO - Dec 2025
- Third-party pen-testing - Jan 2026
- Automated message screening - Q1 2026
- Signature-based anomaly detection - Q2 2026
- SOC 2 - Apr 2026
- ISO 27001 certification - Q4 2026

Mobile Commons has shared these plans with and have collaborated with CTIA Security, InfoBip Security (aggregator), and Mobile Carrier Security teams to validate that the security measures and mitigations are in line with industry best practices.

Mobile Commons takes the security and integrity of its platforms extremely seriously, and are committed to maintaining the customers' trust and will continue to invest in the systems and practices necessary to protect their communications.