ZEROFOX INTELLIGENCE

Flash

Online Impersonations Likely to Spike in July

F-2026-06-30a

Classification: TLP:CLEAR

Criticality: HIGH

Intelligence Requirements: Impersonations, Fraud, Social Engineering

June 30, 2026

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 7:00 AM (EDT) on June 30, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Online Impersonations Likely to Spike in July

| Key Findings

- ZeroFox assesses that impersonation volume is likely to spike in July 2026, consistent with our observed seasonal patterns in the previous reporting period.
- Between May 1, 2025, and April 30, 2026, ZeroFox executed 1,412,243 client-requested takedowns across all monitored network categories, which represents a significant volume of disruption activity on behalf of its customer base.
- ZeroFox observed a significant peak in impersonation volume in Q3 2025, with July 2025 recording the highest single-month total of 191,078 takedowns. This figure was driven predominantly by social media activity, which accounted for the largest share of our takedown submissions throughout the year.
- Following the summer 2025 peak, ZeroFox noted a gradual decline in our overall takedown volume through the fall before a secondary elevation in December 2025. Notably, this was driven by an anomalous spike in peer-to-peer (P2P) and communications activity—a category that otherwise tracked at moderate and relatively stable volumes.

Preliminaries

- A targeted network takes down impersonating content when the impacted individual or entity submits enough convincing evidence of a suspected impersonation.
- All ZeroFox takedowns are client-requested and acted upon accordingly.
- The time period between our client's initial takedown request and the removal of the impersonation account or website varies depending on multiple factors, including acceptance time, collation of evidence of an impersonation, and response time from the targeted network/providers.
- The data analyzed in this report is strictly ZeroFox client-specific and should not be treated as exhaustive but likely reflects identity fraud and impersonation trends in the wider digital space.
- Unlike traditional ransomware and digital extortion (R&DE) operations in which perpetrators can typically be identified based on similarities in root domains or infrastructure, identifying the threat actors behind impersonations on social media networks is very uncommon.
- Network categorization:
  - Domains: domain, surface web, and advanced web search
  - Social: Facebook, Instagram, X, Pinterest, Bluesky, TikTok, and YouTube
  - P2P/Comms: Telegram, phone numbers, and email addresses
  - Others: Everything else (includes Meta Ads, Pastebin, and similar platforms)

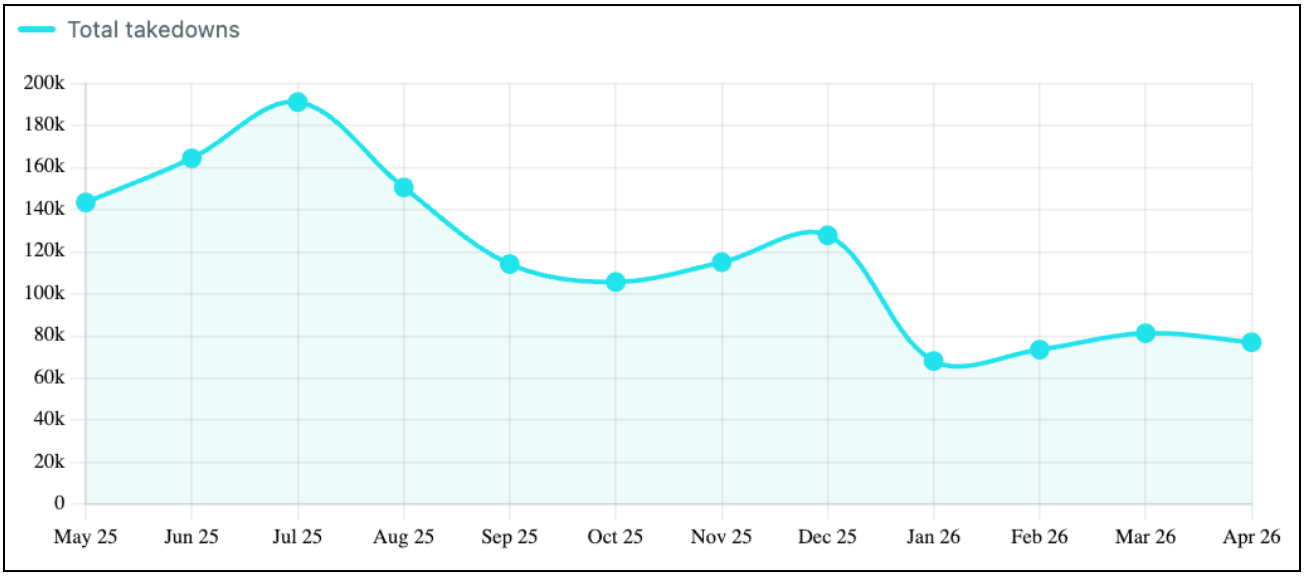
Overview

TOTAL TAKEDOWNS	PEAK MONTH	SOCIAL MEDIA	AVG. MONTHLY
1,412,243	191,078	798,250	117,687
May 2025 – Apr 2026	Jul 25	Largest category	All categories

Between May 1, 2025, and April 30, 2026, ZeroFox executed 1,412,243 client-requested takedowns across all monitored network categories, which represents a significant

volume of disruption activity on behalf of its customer base. We observed a significant peak in Q3 2025, with July 2025 recording the highest single-month total of 191,078 takedowns. This figure was driven predominantly by social media activity, which accounted for the largest share of all submissions throughout the year. Social media platforms collectively represented the majority of the monthly takedown volume across the reporting period, reflecting the continued concentration of impersonation and brand abuse activity across consumer-facing networks.

- Increases and spikes in takedown requests very likely reflect an increase in impersonations in the wider digital space.



ZeroFox takedowns by month

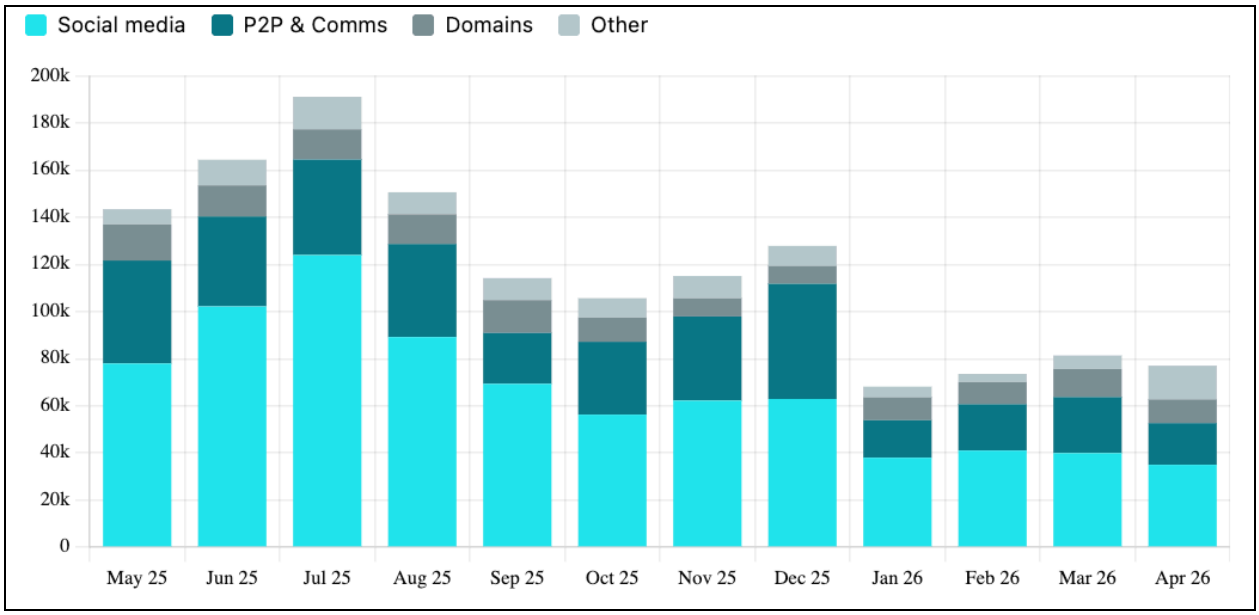
Source: ZeroFox Intelligence

Trends and Observations

Following the summer 2025 peak, ZeroFox noted a gradual decline in the overall takedown volume through the fall before a secondary elevation in December 2025. Notably, this was driven by an anomalous spike in P2P and communications activity—a category that otherwise tracked at moderate and relatively stable volumes. This spike likely reflects a discrete campaign or coordinated impersonation effort routed through messaging platforms and phone-based channels during the holiday period. Since January 2026, ZeroFox has noted a sharp contraction in takedown volume across all categories simultaneously, with monthly totals falling to roughly one third of the July 2025 peak. Domain takedowns remained the most consistent category throughout,

showing less volatility than social or P2P channels. The "Others" category—encompassing Meta Ads, Pastebin, and similar platforms—remained a small but persistent share of activity, with a notable uptick in April 2026 that warrants monitoring going forward.

- The July 2025 peak is consistent with established seasonal patterns in impersonation activity. Elevated consumer engagement across digital platforms during summer months expands the available target population for threat actors operating at scale. Higher social media activity—almost certainly driven by peak vacation time and greater brand visibility across financial and retail verticals due to summer sales and increased lender advertising—collectively lower the barrier for impersonation campaigns to yield returns. ZeroFox assesses the concentration of finance and federal takedowns—the two sectors with the highest takedown volume across the full reporting period—was almost certainly a contributing factor to the July 2025 peak, as both categories attract sustained abuse independent of season. The elevated summer volume should be treated as a planning benchmark rather than an anomaly.
- The anomalous December 2025 spike in P2P and communications activity likely reflects a discrete, coordinated campaign routed through messaging platforms and phone-based channels during the holiday period. P2P impersonation is operationally distinct from domain or social media abuse; it reaches individuals directly over personal communication channels at a time of elevated transaction activity and reduced scrutiny. Targets are likely to include consumers expecting delivery notifications, financial alerts, or government communications—all high-frequency contact types in December. The holiday timing is almost certainly deliberate. Threat actors very likely exploit predictable increases in legitimate communications volume to reduce the likelihood of recipients identifying fraudulent contact.



ZeroFox monthly takedown volume by network type (May 2025–April 2026)
Source: ZeroFox Intelligence

Assessment

Online impersonation volume is likely to spike in July 2026, consistent with seasonal patterns ZeroFox has observed in the preceding reporting period. We assess that the drivers behind the July 2025 peak (elevated social media activity, increased consumer engagement across retail and financial platforms, and sustained abuse targeting finance and federal sectors) will very likely remain structurally present and generate comparable or higher takedown activity in the coming weeks.

Social media will almost certainly remain the dominant impersonation vector in July 2026, as it has across every month of the May 2025–April 2026 reporting period. Peak vacation activity almost certainly expands the available target population; consumer attention shifts toward travel, retail, and financial services, and brand visibility in those verticals increases—conditions that collectively lower the operational threshold for impersonation campaigns to yield returns at scale.

ZeroFox assesses that threat actors will likely prioritize platforms with high consumer-facing traffic (particularly, Facebook, Instagram, and TikTok) as primary deployment channels during this period. Domain-based abuse is likely to run concurrently, consistent with its established pattern as the most stable and persistent

category across the reporting period. P2P and communication channels are unlikely to replicate the anomalous December 2025 spike in July 2026, though a moderate baseline of activity across Telegram and phone-based vectors is likely.

Recommendations

- Monitor owned brand assets across social media platforms, domain registries, and P2P/communication channels continuously to reduce detection latency for impersonation content.
- Establish a documented takedown workflow that defines evidence thresholds, submission processes, and escalation paths by network type to ensure consistent response times across social, domain, and P2P categories.
- Maintain current records of all official brand assets—including social accounts, domains, and executive profiles—to enable rapid identification of unauthorized imitations and support evidence submission to platforms.
- Proactively monitor deep and dark web forums for indicators of impersonation infrastructure, including fraudulent domain registrations, spoofed account templates, and brokered brand assets being prepared for deployment.
- Assess platform response time and acceptance rates as part of vendor evaluation, prioritizing disruption partners with direct relationships with social media networks, registrars, and hosting providers to minimize consumer exposure duration.
- Implement brand protection coverage across emerging and secondary platforms—including messaging applications, Meta Ads, and Pastebin sites, which represent a small but growing share of impersonation activity and may indicate early-stage campaign migration.
- Coordinate with legal and communications teams to define a consumer-facing response posture for active impersonation incidents—particularly in the finance, federal, and retail sectors, where brand trust is the primary threat mechanism.

- Leverage threat intelligence to identify seasonal and event-driven impersonation patterns, and increase monitoring coverage and takedown capacity during high-risk periods such as summer months and the holiday season.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** **TLP:RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** **TLP:AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** **TLP:AMBER+STRICT** restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** **TLP:CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** **TLP:GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** **TLP:CLEAR** information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%