FINTECH INDUSTRY TRENDS, ANALYSIS AND BENCHMARKS

ATTACK PATTERNS REVEALED | RELEASED Q3 2025

ARKOSE LABS

FINTECH INDUSTRY ATTACK POINTS

Fintech platforms recorded the largest relative growth in malicious traffic across all sectors, concentrated in account creation and account management functions. This concentration may reflect the continuing appeal of fintech targets, where successful compromise can yield direct financial benefit or access to verified payment credentials.

Sign-Up Attacks: Substantial Growth

Attacks: +26%	Malicious traffic: +478%	Average attack size: +358%

Sign-up malicious traffic increased more than 17x the industry-wide average (+27%), while attack volume rose modestly. The data indicates a higher level of intensity within each event.

Account Management: Expanded Post-Authentication Activity

Malicious traffic: +302%	Share of attacks: 9% → 17%

Malicious traffic on the account management flow grew more than 4x the cross-industry average (+70%), more than tripling its share of overall fintech activity.

Sign-In: Decline in Line With Market Averages

Malicious traffic: -33%	Industry-wide change: -31%

Sign-in activity declined at a rate similar to the cross-industry averages but remained the dominant attack point, accounting for just above half of all fintech attacks.

What This Reveals

The Q2 data shows heightened emphasis on account-creation and management layers, where growth far exceeded industry baselines. This pattern suggests that attackers perceive increased value in targeting areas tied to verification, credential storage and transactional control.

FINTECH INDUSTRY ATTACK TYPES

The fintech industry saw large shifts in attack behavior in Q2 2025, with spikes in fake account creation and in-app abuse. It's not surprising—fraudsters continue to pursue the quickest path to verified payment credentials and stored financial data.

In-app threats: Expanded Post-Authentication Activity

Attacks: +156%	Malicious traffic: +302%	Average attack size: +57%

In-app threats experienced broad growth across all measures, with traffic rising 5x the in-app threats industry growth of +60%.

Fake Account Creation: Substantial Escalation

Attacks: +19%	Malicious traffic: +659%	Average attack size: +539%

Fake account creation grew at an even faster rate, with malicious traffic surging over sixfold quarter over quarter. The large gap between traffic and frequency points to higher-intensity automation within onboarding flows.

Account Takeover (ATO): Traffic Decline Despite Volume Increase

Attacks: +26%	Malicious traffic: -33%	Average attack size: -47%

Although the number of ATO events increased, the total malicious traffic dropped by one-third. The decline in average attack size suggests smaller-scale credential attacks following Q1's heavier activity.

SMS Toll Fraud: Modest Growth From a Low Base

Attacks: +33%	Malicious traffic: +59%	Average attack size: +19%

SMS-related threats rose across all dimensions but remained a relatively small proportion of total fintech activity.

What This Reveals

Fintech's Q2 data highlights significant pressure on account creation and account management. With fake account creation and in-app threats growing at multiples of the cross-industry growth rate, attackers appear to be concentrating efforts where financial credentials and transaction capabilities are most accessible.

FINTECH INDUSTRY ATTACK MECHANISMS

The tools fraudsters use to execute attacks reveal a surprising inversion of industry trends, with fintech experiencing fundamentally different pressures than other sectors. While bots comprise 61% of all fintech attacks, bot malicious traffic grew just 7% in Q2—far below the industry-wide surge of 22%.

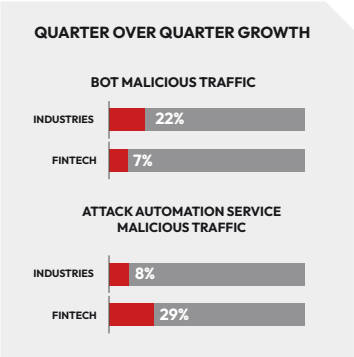
Growth for Attack Automation Services and Human Fraud Farms

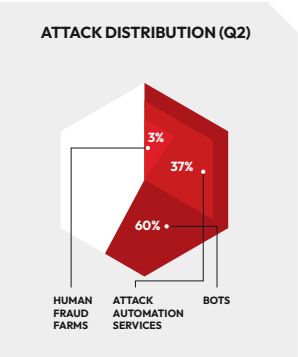
Attack automation services showed moderate but concerning increases. These sophisticated tools grew 29% in malicious traffic, nearly 4x the industry rate of 8%. Despite their share of attacks decreasing from 41% to 37%, attack automation services are generating more traffic per attack.

Another striking finding? Human-operated attacks exploded 231% in malicious traffic, though they remain just 3% of total attacks.

Attack Distribution (Q2)

- **Bots:** 60% (dominant but slower growing)
- **Attack automation services:** 37% (declining share but accelerating traffic)
- **Human fraud farms:** 3% (tiny share but massive growth)





What This Reveals

One possible explanation for the small bot traffic growth? Fintech's bot defenses may be more effective than average, forcing fraudsters to seek alternative methods. Meanwhile, the explosive growth rate for malicious traffic from human fraud farms suggests fraudsters are willing to invest in more resource-intensive attack methods when targeting fintech platforms.

FINTECH INDUSTRY ATTACK BROWSERS & DEVICES

Browser patterns in attacks reveal notable consolidation, with Chrome maintaining overwhelming dominance while mobile browsers show significant growth.

Notable Browser Findings

- In Q2, top 3 browsers account for 79% of all attacks
- Chrome Mobile, Mobile Safari and Chrome Webview showed strong growth
- Several Q1 browsers (Battle.net, WeChat, Headless Chrome) disappeared entirely

Device Distribution Shifts Toward Mobile

- **Attacks via desktop:** Grew 24%
- **Attacks via mobile:** Surged 57%
- **Device distribution:** From 62% desktop/38% mobile to 56% desktop/44% mobile

This 6 percentage point swing toward mobile contrasts with the industry-wide pattern of approximately 68% desktop/32% mobile with minimal quarter-over-quarter change.

What This Reveals

The surge in mobile-originated attacks—more than double desktop's growth—signals fraudsters are expanding mobile attack infrastructure and investing in tools that mimic mobile app traffic patterns.

TOP 5 BROWSERS BY NUMBER OF ATTACKS VIA DESKTOP AND MOBILE DEVICES – FINTECH INDUSTRY, Q2 2025

No.	Desktop Browsers
01	Chrome
02	Firefox
03	Safari
04	Microsoft Edge
05	Chrome Mobile

No.	Mobile Browsers
01	Chrome Mobile
02	Mobile Safari
03	Chrome Webview
04	Chrome
05	Chrome Mobile iOS

FINTECH INDUSTRY ATTACK COUNTRY PATTERNS

Attack geography data reveals that Great Britain dominates fintech attacks at nearly 44% of total volume, with the United States showing surprisingly low representation at just under 13%—a stark contrast to the typical U.S. dominance seen across other industries.

When examining the geographic distribution, several distinct patterns emerge.

Great Britain Dominance: Great Britain's exceptional share represents an unusual concentration for fintech attacks. This may reflect its position as a global financial hub, making these IP addresses attractive for fraudsters targeting financial services.

The U.S. Anomaly: The United States shows dramatically lower attack volumes than the industry norm where U.S. traffic typically dominates. This suggests fraudsters may be using different location-masking strategies when targeting fintech versus other sectors.

South Asian Presence: Pakistan emerges as the third-largest source of attacks, representing a significant concentration relative to its typical presence in other industries.

Global Distribution: The data shows attacks originating from a wide range of countries, indicating a globally distributed threat landscape with fraudsters operating from diverse locations spanning Europe, Asia, Africa and the Americas.

Fintech Industry: Top 10 Attack Origins	
	Great Britain
	United States
	Pakistan
	Brazil
	Algeria
	Germany
	Vietnam
	Kenya
	Ukraine
	Netherlands

FINTECH INDUSTRY RECOMMENDED ACTIONS

Harden Account Creation

Deploy multi-layered verification at sign-up that scales with risk signals. The 478% surge in demands enhanced KYC measures including document verification, biometric checks and behavioral analysis during onboarding.

Counter Fake Account Explosion

Implement graph-based fraud detection to identify connected accounts, deploy velocity checks on payment method reuse and monitor for synthetic identity patterns across your platform.

Secure Mobile Channels

Given the growth in mobile-originated attacks, implement advanced device fingerprinting to detect emulators and device farms. Monitor for browser anomalies that signal attack tool usage.

Geographic Intelligence

Use risk-based authentication that considers geographic patterns—Great Britain leads at 44%, with Pakistan also showing disproportionate activity at 11%.

Maintain Authentication Vigilance

While ATO decreased 33% in malicious traffic, it represents 54% of all fintech attacks. Deploy risk-based MFA, continuous authentication and behavioral anomaly detection to preserve defensive gains.

CONCLUSION

The goal isn't simply to detect and block attacks—it's to make cybercrime unprofitable. When fintech platforms implement adaptive security that scales friction with risk and deploy behavioral biometrics that distinguish humans from sophisticated automation, they actively disrupt the economics that make fraud operations viable. By understanding the scammer behavior, timing patterns and tactical preferences revealed in this infobrief, fintech teams can move from reactive security to proactive defense—protecting not just accounts and transactions, but the trust that forms the foundation of digital banking.

ABOUT ARKOSE LABS

Arkose Labs is the leading global provider offering a proactive fraud deterrence platform purpose-built to neutralize modern attacks, including those powered by Agentic AI and large language models (LLMs). Its comprehensive solution combines proprietary device identification (device ID), behavioral analysis, phishing protection, email intelligence, scraping prevention, API defense and bot management. Trusted by the world's leading consumer brands—including two of the top three banks, Microsoft, Meta, Roblox, and many others—Arkose Labs stops account takeovers, fake account creation, LLM-driven scraping and SMS toll fraud. The platform actively undermines attacker ROI by introducing dynamic friction, making it economically unsustainable for adversaries to persist. Its Security Operations Center (SOC) provides actionable insights from an extensive cross-industry intelligence network, which monitors legitimate traffic and attack patterns across global enterprises. With unparalleled proactive support for internal security teams, Arkose Labs goes beyond conventional security by actively partnering with customers to disrupt organized fraud networks such as Storm-1152. Headquartered in San Mateo, California, the company maintains a global presence with offices throughout APAC, Central America, EMEA and South America.

USA (San Mateo)

Australia (Brisbane)

United Kingdom (London)

Costa Rica (San José)

India (Pune)

Argentina (Buenos Aires)

Book a Meeting