# Shufti Whitepaper Outlines How Deepfakes and Phishing Kits Are Driving a New Wave of Account Takeover Fraud

*A new report from Shufti shows how synthetic identities, credential stuffing, and session hijacking are fuelling account takeover fraud and how to stop it.*

Shufti ATO Whitepaper

LONDON, UNITED KINGDOM, November 19, 2025 / EINPresswire.com/ -- Shufti, the global identity verification provider, has released a new whitepaper outlining how account takeover (ATO) fraud has evolved from a technical vulnerability into a systemic business risk undermining digital trust across financial services, e-commerce, and online platforms.

Titled “Preventing Account Takeover Fraud with Multilayered Defense,” the whitepaper presents ATO not as an isolated technical breach but as the backbone of modern financial crime, fueling everything from unauthorized transfers to phishing scams and social media impersonation.

> “Optimizing ATO defenses needs more than isolated controls. Our risk-adaptive framework unites device fingerprinting, MFA, anti-spoofing, and a network intelligence layer to spot high-risk activity.”
>
> *Shahid Hanif, CEO of Shufti*

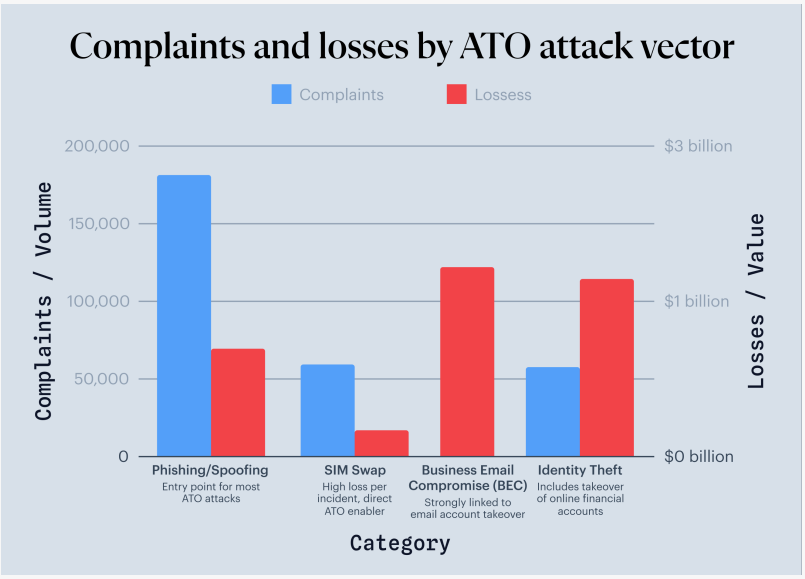
Drawing from Europol’s 2024 IOCTA, FBI IC3 reports, European Banking Authority guidance, and real-world case studies, the report outlines how phishing, synthetic identities, malware, and deepfakes are enabling attackers to bypass weak authentication systems. As accounts are hijacked and reused across digital platforms, businesses face increased liability, reputational harm, and user attrition.

In 2024 alone, U.S. cybercrime losses exceeded $16.6 billion, with a significant share attributed to identity theft and account compromise. As fraud accelerates through phishing-as-a-service,

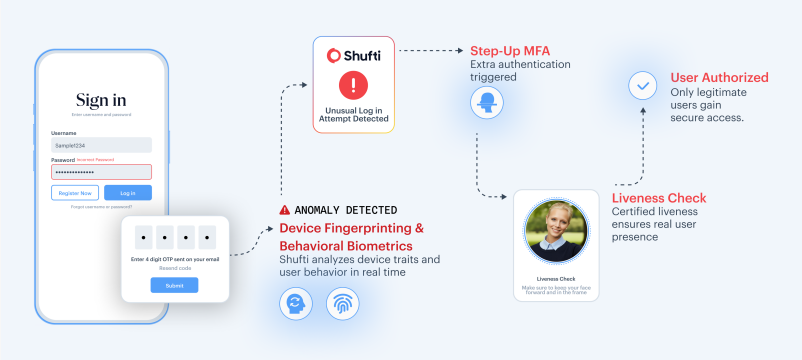
malware kits, and spoofed biometric exploits, businesses are urged to reassess their defense strategies.

The paper outlines how deepfake technology, phishing-as-a-service (PhaaS), and credential theft are escalating the threat beyond traditional MFA defenses.

"Account takeover isn't just about stolen credentials; it's about taking over the user's ongoing session and behavior," said Shahid Hanif, CEO of Shufti. "Fraudsters now mimic legitimate devices and interaction patterns, making static ID checks and one-time KYC fail. Digital trust must be reinforced at every touchpoint through continuous, context-aware authentication that adapts to behaviour and emerging threats, disrupting the fraud lifecycle instead of relying on more ID checks."




Shufti Data- Complaints and losses by ATO




Shufti Risk Adaptive Layered Verification

According to the report, four key trends are driving ATO's growth:
-Credential Leaks: Mass-scale data breaches have created a steady supply of stolen logins.
-Weak Password Hygiene: Reused credentials allow fraudsters to target multiple platforms at once.
-Social Engineering: Sophisticated phishing and impersonation attacks are now accessible even to low-skilled criminals.
-Device Hijacking: Techniques like SIM swapping and session hijacking exploit weak device-level defenses.

The threat is compounded by the emergence of scalable toolkits. Phishing-as-a-service (PhaaS) platforms offer pre-built phishing kits and fake login pages, enabling attackers to launch thousands of simultaneous ATO campaigns. Meanwhile, deepfake generation tools are bypassing liveness detection through manipulated videos and synthetic identities.

The report highlights that traditional MFA is increasingly inadequate in the face of these threats. A facial scan alone, for example, may be vulnerable to spoofing, masks, or injected deepfake

streams.

Shufti's research echoes regulatory consensus that static verification mechanisms are no longer sufficient. Referencing guidance from the Federal Financial Institutions Examination Council (FFIEC) and the EBA–ECB Payment Fraud Report, the whitepaper emphasizes that risk-based, multi-factor authentication and behavioral intelligence are now baseline expectations, not advanced controls.

Verification methods must adapt in real time, correlate multiple signals, and escalate to stronger identity proofing without sacrificing user experience. To address these failures, the paper outlines  Shufti's multilayered fraud prevention framework, a "Unified Defense Strategy" that blends onboarding integrity with continuous fraud monitoring and intelligent account recovery.

Shufti's recommended framework includes:
-Device Fingerprinting: Mapping browser, OS, hardware traits, and session behaviour to the rightful user.
-Behavioral Biometrics: Analysing typing cadence, navigation patterns, and cursor behaviour for passive authentication.
-Liveness + PAD Detection: Blocking spoofing, injection attacks, and synthetic media through skin texture, eye movement, and depth analysis.
-Knowledge-Based and Signal-Aware Recovery: Using correlated verification signals, facial match, document recheck, behavioral fingerprint, to securely return access to compromised users.

The paper also presents sector-specific use cases. In fintech, phishing-driven ATO often leads to unauthorized transfers and fraudulent loan applications, while affected users face immediate financial harm and trust erosion.

In social commerce, compromised accounts are weaponized to distribute phishing links, impersonate brands, or scam followers, damaging both user safety and platform reputation.

The whitepaper highlights that no sector is immune. ATO now spans financial institutions, online marketplaces, and communication platforms. Between 2021 and 2023, account takeover incidents rose dramatically across account types, banking (32% to 42%), social media (51% to 53%), email and messaging platforms (26% to 23%), and e-commerce (8% to 17%), according to data cited.

Shahid Hanif - The CEO of Shufti, further adds;
"Strengthening ATO defence requires more than isolated controls. That's why we've built in-house a risk-adaptive verification framework that delivers a unified, layered defence combining device fingerprinting, behavioural biometrics, advanced MFA, anti-spoofing measures and a network intelligence layer that monitors activity patterns for suspicious or high-risk behaviour. With robust ID verification and recovery processes, it protects users across onboarding and daily

interactions without adding friction for legitimate customers."

To underscore this point, the report references the European Banking Authority's 2024 Payment Fraud Report, which found that transactions authenticated via strong customer authentication (SCA) methods have dramatically lower fraud rates. This reinforces the need for businesses to shift from reactive patchwork defenses to proactive identity assurance frameworks.

Ultimately, the whitepaper frames account takeover as a test of digital trust. In a landscape where users are vulnerable, devices are compromised, and credentials are traded in real time, only platforms that can continuously verify and recover user identity at every step will succeed.

The full whitepaper, Preventing Account Takeover Fraud with Multilayered Defense, is available here:
https://shuftipro.com/resources/whitepapers-reports/preventing-account-takeover-fraud-with-multilayered-defense/

About Shufti
Shufti is a global leader in identity verification and fraud prevention, supporting over 1,000 clients across 240+ countries and territories. Its in-house verification engine combines biometric authentication, document validation, device fingerprinting, behavioral analytics, and real-time orchestration to detect and block fraudulent identities across the user lifecycle.

Shufti's multilayered architecture powers age verification, ATO protection, AML screening, and reusable digital identity frameworks for startups, enterprises, and regulators alike, ensuring secure, compliant, and seamless user journeys. Recognized for innovation and trusted globally, Shufti enables digital trust at scale.

SOURCE SHUFTI

Neliswa Mncube
Shufti
+44 1225 290329
email us here
Visit us on social media:
LinkedIn
Bluesky
Instagram
Facebook
YouTube
TikTok
X