CTX-ADV-2026-1107: Ciphertronix Security Advisory

AI-Enabled and Automated Cyber Threats Targeting Banks and Financial Institutions

Advisory Ref.	**CTX-ADV-2026-1107**	**Date of Issue**	7 November 2026
Severity	■ **HIGH**	**Classification**	TLP:CLEAR
Audience	Commercial, Islamic and microfinance banks, DFIs, PSOs/PSPs and fintech partners	**Reference**	National CERT Advisory NCA-26.051126

1. Executive Summary

Ciphertronix Security Operations is issuing this advisory to its banking and financial sector clients and partners following a marked rise in the use of Artificial Intelligence (AI), automated bots, botnets and agentic tooling by threat actors. These capabilities allow attackers to perform reconnaissance, discover vulnerabilities, test stolen credentials and launch coordinated attacks at a scale and speed that conventional, manually tuned controls were not designed to withstand.

The National Cyber Emergency Response Team (National CERT) of Pakistan has separately highlighted financial services as a sector requiring particular attention. Ciphertronix recommends that every institution reviews the indicators in Section 3 and completes the **immediate actions** in Section 4 as a matter of priority.

2. Threat Landscape for Banks

Based on current threat intelligence and our own assessment and monitoring engagements, the following attack scenarios are considered most relevant to banks and financial institutions:

- **Automated credential attacks:** large scale credential stuffing and password spraying against internet banking, mobile applications and staff portals, using bot networks that rotate IP addresses and imitate genuine user behaviour.
- **API and integration abuse:** automated enumeration of open banking, mobile and partner APIs to locate weak authorisation, excessive data exposure or unprotected endpoints, including those of third party and fintech integrators.
- **Data integrity and balance manipulation:** tampering with customer facing systems so that displayed balances or transaction histories differ from core banking records. Even where funds are unaffected, this may trigger customer panic, complaints and reputational damage.
- **AI-generated social engineering:** highly convincing phishing emails, WhatsApp and SMS messages, cloned voices and video used to impersonate executives, treasury staff, regulators or vendors in order to authorise payments or harvest credentials.
- **Disruption of digital channels:** bot-driven and volumetric denial of service against internet banking, payment gateways, ATM and card switching interfaces, and customer contact centres.
- **Payment system targeting:** unauthorised access to payment, SWIFT, RAAST, IBFT and card management environments through compromised privileged accounts or remote access paths.

3. Indicators and Anomalies to Monitor

Security, fraud and IT operations teams should actively watch for the following indicators and escalate any occurrence through the institution's incident response procedure:

Area	Indicators of Concern
Authentication	Spikes in failed logins, repeated authentication failures across many accounts, logins from unusual ASNs, hosting providers or geographies, and unusual OTP request volumes.
APIs and Applications	Unusual API call patterns or volumes, requests to undocumented endpoints, unexpected changes to application or gateway configuration, and abnormal error rates.
Transactions	Abnormal transaction velocity, beneficiary additions followed by rapid transfers, and many small value test transactions across accounts.
Data Integrity	Mismatches between core banking records and balances shown on internet banking, mobile applications or statements; failed or unexplained reconciliation breaks.
Privileged Access	Access to payment systems, databases or administrative consoles outside approved windows, new privileged accounts, and remote sessions from unrecognised vendor connections.
Communications	Reports of urgent payment or credential requests appearing to come from executives, regulators or vendors, particularly through WhatsApp, voice calls or newly registered domains.

4. Recommended Actions

4.1 Immediate (within 7 days)

- Enforce multi-factor authentication on all customer channels, remote access, email and privileged accounts; remove any exemptions that are no longer justified.
- Enable bot management, rate limiting and anomaly based throttling on internet banking, mobile and API gateways.
- Review and restrict third party and vendor remote access; disable dormant accounts and unused VPN profiles.
- Brief staff, particularly finance, treasury and branch operations, on AI-generated phishing and voice impersonation, and reinforce call-back verification for any payment instruction.
- Confirm that security logs from core banking, payment systems, firewalls and identity platforms are being collected, retained and monitored.

4.2 Short Term (within 30 days)

- Conduct a security assessment of core banking interfaces, APIs, payment gateways, digital banking applications and third party integrations.
- Implement automated integrity checks and independent reconciliation between customer facing systems and core banking records.
- Strengthen privileged access management, including session recording, just-in-time access and periodic access recertification.
- Tune fraud monitoring rules to detect bot-driven activity, credential stuffing outcomes and abnormal transaction velocity.

4.3 Ongoing

- Maintain a regular cycle of vulnerability assessment and penetration testing, with prompt remediation of findings.

- Apply security updates promptly across servers, network devices, endpoints and applications.
- Test incident response, business continuity and customer communication plans against scenarios such as balance display manipulation and digital channel outages.
- Report suspected incidents through the relevant regulatory and national cyber security channels, including the State Bank of Pakistan and National CERT, in line with applicable requirements.

5. How Ciphertronix Can Assist

Ciphertronix supports banks and financial institutions in preparing for and responding to these threats through the following services:

Service	Scope
Vulnerability Assessment and Penetration Testing	Internet banking, mobile applications, APIs, payment interfaces and external perimeter, including bot and automation resilience testing.
Security Architecture and Controls Assessment	Review of network segmentation, privileged access, remote access, logging and monitoring against recognised frameworks and regulatory expectations.
Fraud and Transaction Monitoring	eSentinel EFRMS for real time detection of abnormal transactions, account takeover patterns and mule activity.
Compromise Assessment and Incident Support	Log and endpoint review to identify signs of existing compromise, with containment and recovery guidance.
Awareness and Simulation	Phishing and social engineering simulations and targeted awareness sessions for high risk staff.

Disclaimer: *This advisory is provided for information purposes to assist institutions in strengthening their security posture. It is based on information available at the date of issue and does not constitute a complete assessment of any specific environment. Institutions should evaluate the recommendations against their own risk profile, policies and regulatory obligations. Ciphertronix accepts no liability for actions taken or not taken on the basis of this advisory.*

CIPHERTRONIX
ACCENTUATED TECHNOLOGY