INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-24 13:32 UTC

HuiOne Ecosystem Persists: 30+ Successor Markets Emerge After DOJ Seizure and Treasury Sanctions

THREAT ACTOR | HIGH | CVSS 7.5

SCC Item ID	SCC-TAC-2026-0030
Type	Threat Actor
Severity	HIGH
CVSS Base Score	7.5
Affected Products	HuiOne Guarantee (Haowang Guarantee), H-Pay Service PLC, Prince Group, no specific enterprise software products affected; targets are financial institutions, cryptocurrency platforms, and individual fraud victims globally
Published	2026-06-24T04:55:12
Discovery Source	Rss

Executive Summary

The U.S. Department of Justice seized cloud infrastructure tied to HuiOne Group subsidiaries, and the Treasury Department sanctioned 35 individuals and entities connected to Cambodia's Prince Group transnational criminal organization. HuiOne Guarantee, one of the largest documented illicit online marketplaces, processed over $31 billion in cryptocurrency transactions and provided fraud-as-a-service infrastructure enabling investment fraud, deepfake social engineering, and human trafficking at scale. Despite enforcement action, Flare research identifies more than 30 successor markets already operating, meaning the criminal supply chain that targets financial institutions, cryptocurrency platforms, and individual investors remains active and resilient.

Technical Analysis

HuiOne Guarantee operated as a full-service crimeware supply chain hosted on proprietary encrypted messaging infrastructure, processing over $31 billion in cryptocurrency across its lifecycle. The ecosystem offered modular fraud tooling: spoofed identity documents, deepfake generation services for social engineering, money laundering rails through H-Pay Service PLC, and victim recruitment pipelines feeding pig butchering investment scams. MITRE ATT&CK techniques in use include T1588 (Obtain Capabilities), T1583 (Acquire Infrastructure), T1656 (Impersonation), T1566 (Phishing including T1566.003 spearphishing via service), T1598 (Phishing for Information), T1036 (Masquerading), T1020 (Automated Exfiltration), T1090/T1090.003

(Proxy/Multi-hop Proxy), T1588.001 (Malware acquisition), T1583.006 (Web Services acquisition), and T1588.006 (Vulnerabilities acquisition). CWE-287 (Improper Authentication) and CWE-1390 (Weak Authentication) are contextually relevant to the identity fraud and account takeover vectors this supply chain enables. No CVE applies; this is criminal infrastructure intelligence, not a software vulnerability. Post-seizure, operators have migrated to proprietary encrypted platforms, and 30+ successor markets are documented as active (per Flare Intelligence reporting). FinCEN has designated HuiOne Group a primary money laundering concern and barred it from the U.S. financial system. No patch exists; defensive posture relies on fraud detection, KYC controls, and transaction monitoring.

Action Checklist

1. Step 1: Containment, Screen all inbound transaction counterparties against OFAC's SDN list for the 26 newly sanctioned entities and nine individuals linked to Prince Group and HuiOne subsidiaries. Block or freeze transactions pending review where matches are identified. (NIST AC-3: Access Enforcement; NIST AC-4: Information Flow Enforcement)
2. Step 2: Detection, Audit cryptocurrency transaction logs and wire transfer records for flows routed through known HuiOne-linked wallet addresses published by FinCEN and Treasury. Monitor for deepfake-assisted onboarding attempts: flag KYC submissions with inconsistent liveness detection signals, synthetic document metadata, or identity attributes that match known spoofed document patterns. (NIST AU-6: Audit Record Review, Analysis, and Reporting; NIST AU-2: Event Logging; CIS 8.2: Collect Audit Logs)
3. Step 3: Eradication, Remove or suspend any vendor, payment processor, or correspondent banking relationship that cannot demonstrate clean OFAC screening results against the current HuiOne/Prince Group sanctions list. Revoke API access or service integrations tied to H-Pay Service PLC or affiliated payment infrastructure. (NIST AC-2: Account Management; CIS 6.2: Establish an Access Revoking Process)
4. Step 4: Recovery, Validate that transaction monitoring rules are tuned to flag multi-hop cryptocurrency flows consistent with T1090.003 (Multi-hop Proxy via anonymizing services). Re-run KYC records for high-value accounts onboarded via asynchronous or automated identity verification against updated deepfake detection tooling. Monitor for re-emergence of successor markets by tracking Telegram and encrypted platform channels identified in Flare and Elliptic reporting. (NIST AU-6: Audit Record Review, Analysis, and Reporting for monitoring continuity; Local Account Monitoring; System File Analysis for document verification pipeline integrity)
5. Step 5: Post-Incident, Conduct a control gap review of authentication and identity verification workflows against CWE-287 and CWE-1390 exposure. Assess whether KYC pipelines can detect AI-generated identity documents and deepfake liveness spoofing. Brief fraud operations teams on pig butchering social engineering patterns using T1656 (Impersonation) and T1566 (Phishing) as the primary initial access vectors. Document findings and update fraud-as-a-service threat model. (NIST AC-1: Policy and Procedures; CIS 7.1: Establish and Maintain a Vulnerability Management Process; Multi-factor Authentication for customer-facing account controls; Credential Rotation for any accounts with potential exposure)

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to BSA Officer, General Counsel, and CISO if any transaction match against the HuiOne/Prince Group SDN entries is confirmed processed (not merely flagged), if KYC re-review identifies accounts already onboarded via confirmed deepfake liveness bypass, or if cumulative exposure to sanctioned entities meets your institution's SAR mandatory filing threshold — any of these conditions triggers potential OFAC enforcement liability and FinCEN SAR filing obligations within 30 days of detection.
Recovery Notes	After containment and eradication, maintain enhanced transaction monitoring on all accounts onboarded during the period 2021–2024 when HuiOne Guarantee was at peak operational volume, given the 30+ successor markets confirmed by DOJ to have emerged post-seizure and the documented continuity of fraud-as-a-service infrastructure under new branding. Re-verify correspondent banking relationships quarterly against updated OFAC SDN data for a minimum of 12 months, as Treasury has signaled continued designation activity against Prince Group-affiliated entities. Monitor Flare, Elliptic, and FinCEN advisories for new wallet address clusters associated with HuiOne successor markets and update blockchain analytics watchlists within 24 hours of any new designation.
Forensic Artifacts	Blockchain transaction graph exports (UTXO chains or ERC-20 event logs) showing multi-hop flows through wallet addresses in the Treasury/FinCEN HuiOne designation annexes — the primary artifact linking your institution to sanctioned infrastructure | KYC submission packages (image files, liveness video recordings, device fingerprints, submission IPs, and session tokens) for accounts onboarded via asynchronous or automated identity verification — the forensic record of deepfake-assisted onboarding attempts specific to HuiOne fraud-as-a-service tooling | API gateway access logs for H-Pay Service PLC integration endpoints covering the 90-day pre-designation window — captures transaction laundering patterns and data exfiltration scope attributable to H-Pay's role as HuiOne's payment processing layer | SWIFT MT103 message records and correspondent banking transaction archives for wire transfers routed through Prince Group-affiliated financial entities — required for SAR filing and OFAC enforcement cooperation documentation | Telegram and encrypted platform channel metadata (channel IDs, invite links, message timestamps) associated with HuiOne successor market recruitment activity identified in Flare and Elliptic reporting — establishes the threat actor's continued operational presence post-DOJ seizure

Per-Action IR Details

Step 1: Containment — Screen all inbound transaction counterparties against OFAC's SDN list for the 26 newly sanctioned entities and nine individuals linked to Prince Group and HuiOne subsidiaries. Block or freeze transactions pending review where matches are identified. (NIST AC-3: Access Enforcement; NIST AC-4: Information Flow Enforcement)

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-3 (Access Enforcement), NIST AC-4 (Information Flow Enforcement), CIS 3.3 (Configure Data Access Control Lists)

Compensating: For teams without enterprise sanctions-screening platforms: download the current OFAC SDN list (CSV/XML from ofac.treas.gov) and run a Python or PowerShell name-matching script against your transaction counterparty records daily. Use fuzzy matching (e.g., Python rapidfuzz library) to catch transliterated Khmer-to-Latin name variants common in Prince Group-affiliated entities. Log all matches to a flat file with timestamp, entity name, transaction ID, and amount for manual review queue.

Evidence: Before freezing or blocking any transaction, export the full transaction record including originator wallet address, beneficiary wallet address, transaction hash, timestamp, and any associated IP metadata from your payment

gateway or crypto exchange API. For wire transfers, capture SWIFT MT103 message fields. These records are the primary evidence chain for SAR filing and OFAC enforcement cooperation — freezing without capture loses the metadata needed to establish the transaction graph linking back to HuiOne-affiliated wallet clusters published in Treasury's designation notices.

Step 2: Detection — Audit cryptocurrency transaction logs and wire transfer records for flows routed through known HuiOne-linked wallet addresses published by FinCEN and Treasury. Monitor for deepfake-assisted onboarding attempts: flag KYC submissions with inconsistent liveness detection signals, synthetic document metadata, or identity attributes that match known spoofed document patterns. (NIST AU-6: Audit Record Review, Analysis, and Reporting; NIST AU-2: Event Logging; CIS 8.2: Collect Audit Logs)

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Without a commercial blockchain analytics platform (Chainalysis, Elliptic): load the HuiOne/Prince Group wallet addresses from Treasury designation annexes into a local SQLite database and query your transaction export CSVs using a Python script performing exact-match and one-hop graph traversal (sender → intermediary → sanctioned address). For deepfake KYC detection without enterprise tooling, run submitted identity document images through ExifTool to extract metadata — AI-generated documents frequently exhibit absent or anachronistic EXIF data, uniform DPI inconsistencies, or creation timestamps that postdate the document's purported issue date. Flag submissions where facial liveness video files lack expected device sensor metadata or show frame-rate anomalies consistent with GAN-generated video replay.

Evidence: Capture and preserve: (1) raw blockchain transaction records with full UTXO or ERC-20 event logs before any account action; (2) KYC submission packages including original image files, video liveness recordings, document scans, submission IP address, device fingerprint, and session token from your onboarding platform; (3) API gateway access logs showing the originating IP, user-agent string, and request cadence for KYC submissions — HuiOne-affiliated fraud services have used automated bulk submission patterns identifiable by sub-second inter-request timing; (4) any Telegram channel invite links or referral codes embedded in onboarding flows, which have been documented as HuiOne marketplace recruitment vectors.

Step 3: Eradication — Remove or suspend any vendor, payment processor, or correspondent banking relationship that cannot demonstrate clean OFAC screening results against the current HuiOne/Prince Group sanctions list. Revoke API access or service integrations tied to H-Pay Service PLC or affiliated payment infrastructure. (NIST AC-2: Account Management; CIS 6.2: Establish an Access Revoking Process)

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without an enterprise IAM platform: generate a complete list of active API keys, OAuth tokens, and service account credentials associated with H-Pay Service PLC or any vendor in the Prince Group network from your API gateway management console (e.g., AWS API Gateway, Kong, or equivalent). Immediately rotate your API gateway master credentials, then revoke individual keys by executing a targeted DELETE/PATCH against your gateway's management API. Document the revocation timestamp and confirmation response code for each credential as evidence of timely OFAC compliance action. For correspondent banking relationships, issue formal written suspension notices and retain copies alongside the OFAC designation reference that triggered the action.

Evidence: Before revoking API credentials or suspending vendor integrations, export: (1) complete API access logs for H-Pay Service PLC integrations covering at minimum the 90 days prior to the Treasury designation date, capturing all endpoints called, payloads transmitted, and response codes — H-Pay's role as a payment processor means these logs may contain evidence of transaction laundering patterns; (2) OAuth token issuance and refresh logs from your identity provider showing the full lifecycle of any tokens issued to H-Pay-affiliated service accounts; (3) network flow records (NetFlow/IPFIX) for traffic between your infrastructure and H-Pay API endpoints, preserving source/destination IPs, port numbers, byte counts, and session durations before the integration is severed.

Step 4: Recovery — Validate that transaction monitoring rules are tuned to flag multi-hop cryptocurrency flows consistent with T1090.003 (Multi-hop Proxy via anonymizing services). Re-run KYC records for high-value accounts onboarded via asynchronous or automated identity verification against updated deepfake detection tooling. Monitor for re-emergence of successor markets by tracking Telegram and encrypted platform channels identified in Flare and Elliptic reporting. (NIST SI-4: no mapped control from provided reference — refer to AU-6 for monitoring continuity; D3-LAM: Local Account Monitoring; D3-SFA: System File Analysis for document verification pipeline integrity)

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For successor market monitoring without commercial threat intelligence subscriptions: configure free Telegram monitoring using the Telethon Python library to observe public channels identified in Flare and Elliptic HuiOne reporting for re-emergence keywords (Haowang variants, H-Pay successors, Prince Group-affiliated branding). For KYC re-screening without enterprise deepfake tooling, batch-reprocess previously accepted liveness videos through the open-source FaceForensics++ pretrained detection model or Microsoft's Video Authenticator (free for qualifying organizations) against the account cohort onboarded during peak HuiOne operational periods (2021–2024). Update blockchain transaction monitoring rules in your AML platform to add two-hop and three-hop traversal checks against all wallet addresses from the full Treasury/FinCEN designation corpus, not only direct counterparties.

Evidence: Before re-running KYC pipelines or modifying transaction monitoring rule sets, snapshot: (1) the current state of your transaction monitoring rule configuration (export rule definitions, thresholds, and whitelist/blacklist entries with timestamps) so that pre- and post-remediation detection coverage can be compared in any subsequent audit or regulatory examination; (2) the list of high-value accounts flagged for KYC re-review, including their original onboarding timestamps, submission IP addresses, and verification outcomes — this establishes the remediation scope and timeline; (3) any existing alerts or SAR filings already generated for these accounts, to ensure re-screening findings are appended to the existing case record rather than creating orphaned duplicate investigations.

Step 5: Post-Incident — Conduct a control gap review of authentication and identity verification workflows against CWE-287 and CWE-1390 exposure. Assess whether KYC pipelines can detect AI-generated identity documents and deepfake liveness spoofing. Brief fraud operations teams on pig butchering social engineering patterns using T1656 (Impersonation) and T1566 (Phishing) as the primary initial access vectors. Document findings and update fraud-as-a-service threat model. (NIST AC-1: Policy and Procedures; CIS 7.1: Establish and Maintain a Vulnerability Management Process; D3-MFA: Multi-factor Authentication for customer-facing account controls; D3-CRO: Credential Rotation for any accounts with potential exposure)

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-1 (Policy And Procedures), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For organizations without a dedicated GRC platform: conduct the control gap review using a structured spreadsheet mapping each KYC pipeline step (document ingestion, liveness check, identity attribute matching, manual review escalation) against the authentication assurance requirements in NIST SP 800-63B (freely available). For fraud operations briefing, use the publicly available Sophos 'CryptoRom' and Chainalysis 'Pig Butchering' reports alongside the CISA/FBI joint advisory on investment fraud as no-cost reference materials to build a scenario-based tabletop exercise. Update the threat model in a free tool such as OWASP Threat Dragon, adding HuiOne fraud-as-a-service as an explicit threat actor node with deepfake KYC bypass and multi-hop crypto layering as documented attack paths.

Evidence: Collect and retain for the lessons-learned record: (1) a complete inventory of all SARs filed as a result of this incident, with filing dates and FinCEN acknowledgment receipts, establishing the regulatory response timeline; (2)

documentation of every account suspended, transaction frozen, or vendor relationship terminated, with the specific SDN list entry or wallet address that triggered each action — this is the evidentiary record for any OFAC enforcement inquiry or de-risking audit; (3) pre- and post-incident KYC pipeline configuration exports showing what deepfake detection controls existed at time of exposure versus what was implemented post-review, demonstrating good-faith remediation effort to regulators; (4) the threat model artifact itself, version-controlled with a diff showing what HuiOne/Prince Group-specific threat scenarios were added, for use in future audit and regulatory examination.

Detection Guidance

Financial institutions and cryptocurrency platforms should query transaction logs for wallet addresses and entity names published in the Treasury OFAC SDN update for Prince Group and HuiOne subsidiaries. Monitor for multi-hop transaction chains consistent with T1090.003, cryptocurrency flows that traverse three or more intermediate wallets before reaching a fiat off-ramp are a behavioral indicator. For identity fraud vectors: flag KYC submissions where document metadata does not match expected camera or scanner fingerprints, liveness check response times fall outside human norms, or facial geometry scores cluster near but below rejection thresholds (indicators of deepfake generation, T1656). On the social engineering side, monitor customer service and investment advisory channels for inbound contact patterns consistent with pig butchering: unsolicited romantic or friendship contact leading to investment platform referrals, particularly for platforms not on your approved list (T1566, T1598). Threat intelligence teams should track Telegram channels and proprietary encrypted platforms for successor market advertisements, Flare's research is the current primary source for this signal. FinCEN's designation documents (see T1 sources) contain typology guidance applicable to transaction monitoring rule tuning. Local Account Monitoring and Multi-factor Authentication are relevant countermeasures for account takeover vectors in this supply chain.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`huioneguarantee[.]com (representative; consult FinCEN and OFAC advisories for current active domains)`	HuiOne Guarantee primary marketplace domain — treat all HuiOne Guarantee-affiliated domains as indicative; canonical IOC list published by FinCEN and Elliptic	MEDIUM
URL	`https://www.fincen.gov/news/news-releases/fincen-finds-cambodia-based-huione-group-be-primary-money-laundering-concern`	FinCEN T1 source — contains entity names, typology indicators, and transaction monitoring guidance; use for wallet address and entity name IOC extraction	HIGH
URL	`https://www.regulations.gov/document/FINCEN-2025-0004-0003`	FinCEN Special Measure final rule — authoritative source for regulated entity obligations and covered HuiOne Group entities	HIGH

Framework Mappings

MITRE-ATTACK

- **T1588** — Obtain Capabilities
- **T1583** — Acquire Infrastructure
- **T1656** — Impersonation
- **T1588.006** — Vulnerabilities
- **T1566** — Phishing
- **T1036** — Masquerading
- **T1020** — Automated Exfiltration
- **T1588.001** — Malware
- **T1583.006** — Web Services
- **T1566.003** — Spearphishing via Service
- **T1598** — Phishing for Information
- **T1090** — Proxy
- **T1090.003** — Multi-hop Proxy

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SR-2** — Supply Chain Risk Management Plan
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **15.1** — Establish and Maintain an Inventory of Service Providers

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.312(e)(1)** — Transmission Security

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain
- **A.8.24** — Use of cryptography
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1588	Obtain Capabilities	Resource-Development
T1583	Acquire Infrastructure	Resource-Development
T1656	Impersonation	Defense-Evasion
T1588.006	Vulnerabilities	Resource-Development
T1566	Phishing	Initial-Access
T1036	Masquerading	Defense-Evasion
T1020	Automated Exfiltration	Exfiltration
T1588.001	Malware	Resource-Development
T1583.006	Web Services	Resource-Development
T1566.003	Spearphishing via Service	Initial-Access
T1598	Phishing for Information	Reconnaissance
T1090	Proxy	Command-And-Control
T1090.003	Multi-hop Proxy	Command-And-Control

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/doj-seizes-huione-cloud-account-t...	T3

Source	URL	Tier
FinCEN Finds Cambodia-Based Huione Group to be of Primary ...	https://www.fincen.gov/news/news-releases/fincen-finds-cambodia-bas...	T1
Special Measure Regarding Huione Group, as a Foreign Financial ...	https://www.regulations.gov/document/FINCEN-2025-0004-0003	T1
FinCEN Bars Huione Group from Financial System	https://www.moneylaunderingnews.com/2025/10/fincen-bars-huione-grou...	T3
Huione Guarantee: The multi-billion dollar marketplace used by ...	https://www.elliptic.co/blog/cyber-scam-marketplace	T3

Generated 2026-06-24 13:32 UTC by TJS Security Command Center