EDP ECOSYSTEM DEEP-DIVE

MODULE 14: MULE NETWORKS

Module Number	14
Module Name	Mule Networks
EDP Node Reference	Node 09 (primary): Mule/Money Laundering Networks; cross-linkage Nodes 01, 02
Ecosystem Layer	Fiat Layering and Integration
Upstream Connections	OTC Brokers (Module 12 / Node 01); Money Launderers and Exchanges (Module 13 / Node 02)
Downstream Connections	Integration into legitimate economy: real estate, business fronts, luxury goods, financial instruments
Research Date	April 2026
Primary Researcher	Reno
Source Tools Used	Perplexity AI; KPMG; Outseer/RUSI-based UK mule research; BioCatch; Napier AI; Unit21; Group-IB; TRM Labs
Handling	INTERAGENCY

SECTION 1: WHAT IT IS

Definition and Ecosystem Role

Mule networks are the fiat layering and integration layer of the ransomware supply chain. They operate downstream of the crypto cash-out point — receiving fiat proceeds from exchanges, OTC brokers, or high-risk VASPs and dispersing them across networks of individual mule accounts and shell company structures to obscure origin and create the transactional distance required for integration into the legitimate economy. Node 09 is a Phase C node in the EDP Disruption Playbook, alongside Nodes 05 (Loaders) and 06 (Leak Sites). It represents the terminal stage of the ransomware monetization chain: the point at which criminal proceeds become usable criminal wealth.

Mule networks serve a specialized function that cyber crews are both unable and unwilling to perform in-house. Professional mule operators maintain standing inventories of accounts across multiple banks and jurisdictions, expertise in local AML thresholds and transaction monitoring triggers, and established relationships with integration-stage asset acquisition networks. TRM Labs documents that ransomware and other cybercrime groups outsource the layering and integration function to specialist networks precisely to minimize their direct exposure to banking KYC — maintaining their focus on intrusion and extortion while delegating the financially complex and compliance-exposed downstream work.

The defining operational characteristic of mule networks is velocity. UK research based on 2024 bank data found that over 50% of funds left identified mule accounts within one hour of arrival; in many cases, funds moved within 15 minutes. This speed is the core of the layering function: real-time payment rails (Faster Payments, instant P2P apps) allow criminal proceeds to clear multiple account layers before any transaction monitoring flag can produce an investigative response.

The Three Stages: Placement, Layering, Integration

Placement: Criminal proceeds enter the banking system from the crypto cash-out layer (OTC broker or exchange). This typically occurs via wire transfer from a high-risk VASP or shell company account to initial mule accounts. Placement is the highest-risk stage for detection — it represents the first point of contact between the illicit crypto proceeds and the regulated banking system.

Layering: Sequential electronic transfers disperse placed funds across multiple mule accounts, shell company accounts, and jurisdictions. Common layering methods include: rapid serial transfers between personal and business accounts (smurfing across mule networks); cross-border wires via correspondent banks for round-amount sham invoices or consulting fees; purchasing financial instruments or re-entry into virtual asset ecosystems to add additional transactional layers; and circular payments between controlled entities. The UK data showing >50% of funds leaving within one hour represents the layering stage in operation.

Integration: Layered funds re-enter the legitimate economy via asset acquisition (real estate, vehicles, luxury goods), business acquisition, or pseudo-legitimate income streams (dividends from front companies, loans from criminal-controlled lenders, fake revenue from service businesses). Integration is the lowest-risk stage for detection: by the time funds reach integration, the transactional trail is typically too diffuse and cross-jurisdictional for standard financial intelligence tools to reconstruct.

Scale and Structural Context

[CONFIRMED] BioCatch reported nearly 2 million money-laundering accounts flagged by 257 financial institutions across 21 countries in 2024. This figure represents the supply side of the mule account ecosystem — the standing inventory of controlled accounts available for layering operations at any given time. This scale makes individual-account-level disruption operationally infeasible; effective disruption must target the herder and professional crew tier rather than individual mules.

[ANALYST INFERENCE] The same mule networks that service ransomware cash-out also service fraud, business email compromise, romance scam proceeds, carding, and other cybercrime verticals. This cross-vertical function creates an important disruption multiplier: mule network disruption degrades the post-cash-out infrastructure for the entire cybercrime ecosystem, not just ransomware. This cross-cutting effect should be a primary argument for prioritizing mule network disruption in interagency resource allocation discussions.

SECTION 2: KEY ACTORS AND EXAMPLES

Archetypes and Named Examples

Archetype	Recruitment Method	Account Tier	Velocity / Channel	Integration Function	Confidence
Retail / unknowing mules	Work-from-home scams, romance fraud, "payment processing" job ads via social media and messaging apps	Personal bank accounts; typically single-institution; low per-account volume	Faster Payments, instant P2P apps, ATM cash withdrawals; funds forwarded within minutes	Placement and initial layering only; no integration function; mule unaware of criminal origin	**[CONFIRMED]** High — well-documented typology across multiple jurisdictions
Structured herder networks	Centralized recruitment via Telegram channels, social media ads, and sometimes Google ads (Group-IB UNC2891 case); handlers script timing and routing	Dozens to thousands of mule accounts per network; mix of personal and business accounts; multi-institution	Coordinated disbursement; 57% Faster Payments, 20% debit card, 10% ATM/cash (UK data); >50% of funds out within 1 hour	Mid-tier layering; smurfing across accounts; may feed professional laundering crews for integration stage	**[CONFIRMED]** High — UK bank data, KPMG, Group-IB documentation consistent

Professional laundering crews ("mule factories")	Criminal organization recruitment; operators are knowingly complicit; may supply accounts to multiple crime verticals simultaneously	Shell company accounts, front business accounts, layered across multiple banks and jurisdictions; high per-account volume	Slower, more deliberate layering via wire transfers, sham invoices, trade-based schemes; cross-border moves	Full-service layering and integration: real estate, luxury goods, business acquisition, loan schemes, dividend channels	**[CREDIBLE]** Moderate-High — typology well-documented; specific operator identities rarely public
Group-IB UNC2891 (ATM cash-out network)	Google ads and Telegram posts recruiting mules for ATM cash-out operations; structured herder model	ATM-focused; geographically dispersed; physical cash extraction as primary output	ATM withdrawals at multiple locations; simultaneous cash-out coordinated by central handler	Cash extraction; no fiat integration function; proceeds delivered to handler	**[CONFIRMED]** High — Group-IB operational case study; cross-over between cyber operations and physical cash-out documented

Velocity and Channel Data: UK Mule Network Study

The most granular available dataset on mule network operational behavior comes from 2024 UK banking data analyzed in Outseer/RUSI-based research. The dataset covers £7.2M moved from identified mule accounts over a two-month window.

Channel	Share of Outflows	Operational Notes
Faster Payments (instant bank transfer)	**57%**	Primary layering channel; immediate settlement; no recall window once sent; most difficult for banks to intercept post-initiation
Debit card payments	**20%**	Used for retail purchases, gift cards, and prepaid card loading; converts fiat to semi-liquid assets quickly
ATM / branch cash withdrawal	**10%**	Physical cash extraction; highest anonymity at point of withdrawal; typically used for final delivery to handlers or direct criminal use
Other channels (wire, P2P apps, etc.)	**13%**	International wires for cross-border layering; P2P app top-ups; cryptocurrency re-entry for additional layering
Time to fund exit from mule account	**>50% within 1 hour; <15% remaining after 24 hours**	Illustrates why standard next-day transaction monitoring is largely ineffective; real-time detection is the only viable intervention window

Recruitment Ecosystem

[CONFIRMED] KPMG's "Money Mules: FinCrime's Trojan Horse" documents multi-stage recruitment funnels: social media and messaging app advertising drives prospects to handlers, who then provide scripts specifying how and when to move funds. Mules are told they are processing legitimate payments, working as "financial agents," or acting as "payment processors" for foreign companies. Commission rates of 5-10% of moved funds are standard.

[CONFIRMED] Group-IB's UNC2891 case documented threat actors placing Google ads and Telegram posts to recruit mules specifically for ATM cash-out operations, illustrating the cross-over between cyber operations and

physical cash extraction networks. The use of legitimate advertising platforms (Google Ads) for mule recruitment represents an ongoing platform-governance challenge with direct implications for mule network scaling capacity.

[CREDIBLE] Herder-level operators in structured networks may simultaneously supply mule accounts to multiple cybercrime verticals — ransomware, fraud, business email compromise, carding, romance scam proceeds. This cross-vertical function makes herder disruption more strategically valuable than its ransomware-specific revenue contribution alone would suggest.

SECTION 3: INFRASTRUCTURE DEPENDENCIES

Upstream Dependencies

OTC brokers (Node 01 / Module 12): OTC broker fiat payouts are the primary upstream input to mule networks for high-value ransomware proceeds. After conversion from cryptocurrency, OTC desks initiate wires to mule account clusters directly or via shell company intermediaries. OTC disruption reduces the volume and "cleanliness" of fiat entering mule network pipelines.

Exchanges and money launderers (Node 02 / Module 13): High-risk exchange fiat withdrawals and wire transfers from money laundering networks also feed mule accounts. Exchange off-ramp compliance improvements reduce the volume reaching mule networks via this pathway.

Shell company infrastructure: Mule networks depend on shell company accounts as both receiving entities (placement-stage wires from OTC/exchange arrive at shell company accounts before dispersal to individual mules) and integration vehicles. Shell company formation services are a separate criminal supply chain not currently represented as a dedicated EDP node.

Real-time payment rails (Faster Payments, RTP, SEPA Instant): Mule networks' velocity advantage depends entirely on the availability of real-time payment rails that provide irrevocable, instant settlement. These are regulated infrastructure — engaging payment network operators and their member banks on real-time mule detection is a structural intervention point.

Downstream Dependencies

Real estate sector: Integration via property purchase is the highest-value single integration channel. Real estate provides durable asset storage, legitimate income streams (rental), and resale liquidity. Beneficial ownership registries, enhanced due diligence on cash purchases, and anti-money-laundering requirements for real estate agents are the primary regulatory chokepoints.

Business front companies: Front businesses (bars, logistics companies, retail outlets) generate pseudo-legitimate revenue streams that integrate criminal proceeds as normal trading income. These entities are harder to identify than real estate purchases and require transaction monitoring across the business banking sector.

Luxury goods and financial instruments: High-value moveable assets (vehicles, jewelry, art, precious metals) and financial instruments (insurance policies, investment accounts) provide liquid integration vehicles. Regulatory requirements for luxury goods dealers and high-value asset sellers vary significantly across jurisdictions — creating exploitation opportunities in lower-regulation markets.

Critical Chokepoints

Chokepoint	Description	Primary Owner	Disruption Method
Herder and network coordinator tier	Herders and coordinators are the operational intelligence of structured mule networks; their removal degrades account supply, coordination, and knowledge of AML thresholds across dozens to thousands of individual mules	FVEY LE FOs; national financial crime units (SOCA, BKA, FBI)	HUMINT penetration; undercover operations; financial intelligence referral from bank SAR analysis; prosecution under conspiracy and money laundering statutes

Real-time payment rail intervention	>50% of mule network outflows use real-time Faster Payments and equivalent rails; this is the only intervention window narrow enough to catch funds before they clear multiple layering hops	Payment network operators (Pay.UK, The Clearing House, EBA Clearing); member bank fraud teams	Real-time mule detection models at payment network level; Confirmation of Payee / Verify Name mechanisms; reimbursement liability frameworks that incentivize bank investment in detection
Mule account identification and freeze	Individual mule accounts are the execution layer; mass identification enables account freezing and disruption of active layering operations; coordinated freeze actions across multiple banks simultaneously degrade network capacity	FVEY LE FOs; national financial intelligence units (FinCEN, NCA, Europol); major retail banks	BioCatch and behavioral biometrics for account classification; coordinated LE-industry freeze operations; suspicious activity report analysis at network level rather than individual account level
Google and platform mule recruitment advertising	Google Ads and Telegram are primary mule recruitment channels; platform-level enforcement against recruitment advertising would constrain the account supply pipeline	Private sector (Google, Meta, Telegram); FVEY LE (for platform engagement)	Platform terms of service enforcement; law enforcement referrals for identified recruitment accounts; industry-government working groups on mule recruitment advertising
Integration-stage asset acquisition controls	Real estate, luxury goods, and business acquisition are the primary integration vehicles; enhanced due diligence and beneficial ownership requirements at these chokepoints prevent final laundering completion	FinCEN; FCA; FVEY financial regulators; national AML supervisors	Beneficial ownership registry requirements; cash transaction reporting for real estate and luxury goods; enhanced due diligence for high-risk customer profiles at asset acquisition points

Cross-Module Linkages

Module	Node	Linkage Type	Direction	Description
12 OTC Brokers	01	Primary supply	Upstream	OTC broker fiat payouts are the primary upstream input; OTC disruption directly reduces mule network inflow volume
13 Money Launderers / Exchanges	02	Secondary supply	Upstream	Exchange fiat withdrawals and money laundering network wires also feed mule accounts; exchange compliance improvements reduce this input channel
07 Ransomware / RaaS	Cross-cutting	Indirect supply	Upstream (via OTC/exchange)	Ransomware proceeds drive the entire financial chain; mule networks are the terminal fiat stage of every ransomware payment that reaches cash-out
10 Underground Forums	07	Recruitment	Upstream	Forums host mule recruitment advertising and herder coordination threads; forum disruption degrades the primary structured recruitment channel for professional-tier networks
No dedicated integration node	N/A	Downstream output	Downstream	Mule networks feed directly into the legitimate economy (real estate, business fronts, luxury goods); no EDP node currently covers this stage

SECTION 4: DISRUPTION LEVERAGE POINTS

Primary Leverage Points

Lever	Owner	Best Method	Backfire Risk	EDP Phase
Herder and coordinator prosecution	FVEY LE FOs; national financial crime units (FBI, NCA, BKA, Europol)	HUMINT penetration of herder networks; undercover operations; financial intelligence referral from SAR pattern analysis; prosecution under money laundering conspiracy statutes; asset forfeiture	**LOW-MEDIUM** — herder arrest produces network disruption but may trigger recruitment of replacement; network-level prosecutions more durable than individual arrests	Phase C — primary action; long-cycle
Real-time payment rail mule detection	Payment network operators (Pay.UK, The Clearing House); member bank fraud teams; national payment regulators	Real-time mule classification models at payment network level; Confirmation of Payee / Verify Name friction; reimbursement liability frameworks creating bank financial incentive for detection investment	**LOW**	Phase C — structural; requires regulatory action
Coordinated bank-LE mule account freeze operations	FVEY LE FOs; national financial intelligence units; major retail bank fraud teams	Network-level SAR analysis to identify mule account clusters; coordinated simultaneous freeze across member banks during active layering operations; BioCatch behavioral biometrics integration	**LOW**	Phase C — operational; requires multi-institution coordination
Platform enforcement against mule recruitment advertising	Private sector (Google, Meta, Telegram); FVEY LE engagement	Terms of service enforcement against identified mule recruitment accounts; LE referrals for platform reporting; industry working group on mule recruitment advertising detection	**LOW**	Phase C — compound; degrades account supply pipeline
Rosfinmonitoring and RU financial intelligence pipeline (conditional)	Rosfinmonitoring; CBR; FinCEN bilateral engagement	Financial intelligence referral under existing AML cooperation frameworks; suspicious activity sharing on identified RU-connected mule	**LOW-MEDIUM** — conditional: Rosfinmonitoring cooperation is structurally limited for ransomware-linked flows given RU state	Phase C — conditional; limited utility for RU-origin ransomware

		flows; bilateral joint financial investigation	protection framework; viable only for cases without FSB-adjacency	

Compounding Actions

- Phase A and B financial actions (Nodes 01, 02, 08) compound mule network disruption by reducing the volume and quality of fiat entering the mule pipeline. Fewer OTC-converted funds and tighter exchange compliance means fewer high-value flows for herder networks to process — degrading their revenue and making the criminal business case for maintaining large account inventories weaker.
- Liability framework reform is the highest structural leverage point for real-time rail disruption. Reimbursement liability frameworks — which require banks to compensate mule-facilitated fraud victims unless they can demonstrate adequate fraud controls — create a direct financial incentive for bank investment in real-time mule detection. The UK's Authorised Push Payment (APP) fraud reimbursement framework is the leading model.
- Network-level SAR analysis produces dramatically higher-quality intelligence than individual account-level reporting. Financial intelligence units that can analyze SAR data across multiple institutions simultaneously identify herder-level coordination patterns invisible in single-institution reporting — the key to targeting herders rather than individual mules.
- Cross-vertical disruption effect: any herder network prosecution that disrupts a major structured mule network degrades cash-out capacity for fraud, BEC, carding, and romance scam verticals simultaneously — multiplying the operational disruption value beyond the ransomware-specific calculation.
- Coordinate integration-stage controls with FVEY financial regulators: beneficial ownership registry requirements and enhanced due diligence for real estate and luxury goods transactions are the primary tool for preventing completion of the laundering cycle. These regulatory actions do not require LE cooperation with Russia and are therefore not constrained by the Russian state protection framework.

SECTION 5: RESILIENCE AND REPLACE DIFFICULTY

Replace Difficulty Assessment

Node 09 carries a MEDIUM replace difficulty rating in the EDP Dependency Map — reflecting a genuine internal split between the highly replaceable retail mule tier and the moderately difficult-to-replace herder and professional crew tiers. The key driver of the MEDIUM aggregate rating is account supply: nearly 2 million mule accounts were active in 2024 (BioCatch), providing enormous redundancy at the individual account level. Individual mule arrests and account freezes do not meaningfully reduce network capacity because the recruitment pipeline continuously replenishes the account supply.

Herder-tier and professional laundering crew disruption is more durable because it removes operational knowledge — specifically, expertise in bank-specific AML thresholds, real-time rail timing, cross-border correspondent banking routes, and integration-stage asset acquisition channels. This knowledge is not widely distributed and takes time to rebuild after a network disruption.

Tier	Replace Difficulty	Key Durability Driver	Key Vulnerability	Recovery Timeline
Retail / unknowing mule accounts	**VERY LOW**	Nearly unlimited supply: 2 million accounts active in 2024 across 21 countries; continuous new recruitment from social media and messaging platforms	Real-time behavioral biometrics and account classification can freeze large batches; but recruitment pipeline refills faster than freeze operations	Hours to days for individual account replacement; weeks for network reconstitution after coordinated freeze operation

Structured herder networks	**MEDIUM**	Herder expertise in local AML controls, payment rail timing, and multi-bank coordination is moderately specialized; cross-vertical client base creates revenue stability and operational incentive to maintain capacity	Herder identity exposure via HUMINT or financial intelligence; multi-institution SAR coordination identifies herder-level coordination patterns	Months — herder network disruption takes weeks to months for clients to identify and vet equivalent-quality replacements; transitional period of elevated risk and reduced capacity
Professional laundering crews (shell company and integration tier)	**HIGH**	Shell company networks, banking relationships, real estate acquisition channels, and integration-stage asset networks take years to build; off-chain settlement reduces attribution surface	Rarely identified without HUMINT; asset forfeiture can remove integration-stage holdings; beneficial ownership registries create attribution risk at real estate and business acquisition stage	Years — professional crew disruption is rare; when achieved, clients may have no equivalent alternative and may be forced to accept lower-quality layering or hold proceeds in crypto longer

Historical Reconstitution and Case Record

Operation / Case	Enforcement Action	Date	Outcome	Notes
Europol Operation Eagle II	Coordinated arrests across multiple EU countries; mule account identification and freeze	2024	Hundreds of arrests; thousands of mule accounts frozen; coordinated across 26 countries	Demonstrates viable multi-jurisdiction mule network disruption; but network reconstitution within months is expected at individual account level; herder-level impact not publicly quantified
Group-IB UNC2891 (ATM cash-out network)	Investigation and exposure; operator details shared with LE	2023-2024	Network structure documented; LE referral; specific arrest outcomes not publicly confirmed	Illustrates cross-over between cyber operations (digital recruitment via Google Ads/Telegram) and physical cash-out infrastructure; model for other structured herder networks
FinCEN-led multi-bank mule account freeze operations (US)	Coordinated SAR analysis; simultaneous account freezes across member banks	Recurring	Millions in frozen funds per operation; but individual operations do not degrade network-level capacity sustainably	Network-level SAR analysis approach is directionally correct; scaling this to cross-institutional real-time analysis is the next capability gap

Rosfinmonitoring Pipeline: Structural Limitations

[ANALYST INFERENCE] The EDP Dependency Map identifies Rosfinmonitoring as a co-primary owner of Node 09 disruption via the FNS referral and Rosfinmonitoring pipeline. This reflects the theoretical bilateral financial intelligence cooperation framework. In practice, this pathway is structurally constrained for ransomware-linked mule flows for two reasons: first, Rosfinmonitoring operates under the same Russian state protection framework (Dark Covenant 3.0) that provides implicit tolerance for high-value ransomware operators; second, Russian financial intelligence cooperation on cybercrime has historically been selectively responsive — useful for cases the Kremlin wants actioned, not for cases where the operators are protected. The Rosfinmonitoring pathway should be maintained as a formal channel but not relied upon as a primary disruption mechanism for ransomware-connected mule flows.

SECTION 6: INDICATORS AND KPIs

Ecosystem Health Indicators

Indicator	Normal State (2024-2025 Baseline)	Under Pressure / Degraded
Global mule account inventory (active flagged accounts)	Nearly 2 million accounts flagged across 257 institutions in 21 countries in 2024 (BioCatch)	Year-over-year decline in flagged active mule accounts; sustained decline requires real-time detection improvement, not just reactive freeze operations
Mule fund velocity (time from receipt to outflow)	>50% of funds leaving within 1 hour; <15% remaining after 24 hours (UK 2024 bank data); Faster Payments share at 57% of outflows	Average dwell time increasing above 4 hours indicates real-time detection friction working; Faster Payments share declining indicates detection forcing migration to slower channels
Herder network prosecution rate (FVEY)	Low absolute rate; few publicly documented herder-tier prosecutions versus retail mule arrests; Europol Eagle-series operations most visible	Sustained herder-tier prosecution rate increasing YoY; network-level disruptions rather than individual account freezes
Cross-jurisdiction coordinated mule freeze operations	Annual Europol coordinated operations; Operation Eagle II (2024) involved 26 countries; scope expanding	Operations expanding to cover more institutions and jurisdictions; accounts frozen per operation increasing; time from identification to freeze decreasing
Mule recruitment advertising on Google and Telegram	Active recruitment advertising documented; Group-IB UNC2891 showed operational Google Ads campaigns for mule recruitment	Platform enforcement reducing recruitment ad volume; mule operators shifting to darker channels (private Telegram groups, encrypted messaging only) indicates successful surface-level platform enforcement

Disruption KPIs

KPI	Baseline	Target Under Disruption	Collection Method
Active mule accounts flagged globally (annual)	Nearly 2 million in 2024 (BioCatch, 257 institutions, 21 countries)	Year-over-year decline; below 1.5 million sustained over two consecutive years	BioCatch annual report; national financial intelligence unit aggregate reporting; major bank fraud team data sharing
Average mule fund dwell time before layering exit (hours)	Median below 1 hour; >50% under 60 minutes; <15% remaining at 24 hours (UK 2024 data)	Median dwell time above 4 hours indicates real-time detection friction extending attacker exposure window; sustained above 4 hours signals effective intervention	Payment network operator (Pay.UK, The Clearing House) transaction monitoring data; member bank fraud team aggregate reporting
Herder-tier prosecutions per year (FVEY combined)	Low baseline — few public herder-tier prosecutions versus retail mule arrests; exact baseline requires	Year-over-year increase in herder and professional crew prosecutions versus retail mule arrests; herder-tier prosecution	DOJ, NCA, BKA, Europol prosecution statistics; interagency financial crime reporting

	interagency data compilation	share above 20% of total money mule charges	
Value frozen in coordinated mule network operations (annual, USD equivalent)	Europol Eagle II (2024) and comparable operations; total value not publicly specified but estimated in millions per operation	Annual frozen value exceeding $100M across FVEY coordinated operations; sustained over three consecutive years	Europol press releases; DOJ asset forfeiture reporting; FinCEN SAR aggregate statistics
Real-time payment rail APP fraud reimbursement rate (UK model)	UK APP fraud reimbursement framework implemented October 2023; PSR mandatory reimbursement up to GBP 415,000 per claim	Reimbursement rate below 30% of total APP fraud losses indicates bank detection improving (fewer successful mule transfers); above 50% indicates detection failing and liability costs rising	Payment Systems Regulator annual reporting; UK Finance fraud data; bank quarterly fraud disclosures

Alert Thresholds

Threshold	Trigger Condition	Response
Single herder network identified controlling above 500 mule accounts across 3+ institutions	Financial intelligence analysis or bank fraud team collaboration identifies a single herder or network coordinating above 500 accounts simultaneously	Escalate to multi-institution coordinated freeze operation; initiate LE investigation for herder prosecution; share network topology with FVEY partners for cross-jurisdiction impact
Mule account inventory rebounds above 2.5 million globally	BioCatch or equivalent reporting indicates year-over-year increase above 25% from 2024 baseline of 2 million	Assess whether increase reflects improved detection (more accounts identified, not more accounts existing) or genuine network expansion; cross-reference with Faster Payments outflow data
Ransomware-linked mule flows identified in new jurisdiction or rail	Financial intelligence identifies significant ransomware-linked fiat flows entering a jurisdiction or payment rail not previously associated with ransomware layering	Alert relevant national financial intelligence unit and FVEY partners; assess for new mule network or established network geographic expansion; consider preemptive regulatory engagement with local payment sector
Professional laundering crew identified servicing multiple ransomware groups	HUMINT or financial intelligence links a single professional laundering crew to 3+ active ransomware groups	Escalate to senior FVEY LE coordination; prioritize for prosecution given cross-vertical disruption value; assess Dark Covenant protections before attribution action if RU-based operators

SECTION 7: SOURCES AND CONFIDENCE

Primary Sources

Financial Crime Research and Industry:

- KPMG — "Money Mules: FinCrime's Trojan Horse Unveiled": mule archetypes; multi-stage recruitment funnel documentation; layering and integration role; cross-vertical function of herder networks.
- Outseer / RUSI-based analysis — "Following the Fraud: What New UK Research Reveals About Money Mule Networks": channel mix data (57% Faster Payments, 20% debit card, 10% ATM); £7.2M two-month

sample; velocity data (>50% within 1 hour, <15% at 24 hours); primary quantitative source for mule network operational behavior.

- BioCatch — "Nearly 2 Million Money Laundering Accounts Reported in 2024": global mule account scale (2 million accounts, 257 institutions, 21 countries); primary source for account inventory baseline.
- Napier AI — "What is layering in money laundering?": layering methods and cross-border typologies; definitional framework for placement/layering/integration stages.
- Unit21 — "The 3 Stages of Money Laundering": placement/layering/integration examples across banking and crypto; integration-stage asset typologies.
- Group-IB — UNC2891 money mule network case: Google Ads and Telegram recruitment; structured ATM cash-out network; documented cross-over between cyber operations and physical cash extraction.

Law Enforcement and Government:

- Europol — Operation Eagle II (2024): 26-country coordinated mule network disruption; arrest and account freeze statistics.
- UK Payment Systems Regulator — APP fraud reimbursement framework (October 2023): mandatory reimbursement liability model; structural incentive for bank detection investment.

Blockchain Analytics and Financial Intelligence:

- TRM Labs — "Ransomware in 2024: Latest Trends, Mounting Threats and the Government Response": outsourcing of layering and cash-out functions by ransomware and cybercrime groups; specialist mule network subcontracting model.

Confidence Assessment by Topic

Topic	Confidence Level	Basis	Key Limitations
UK mule fund velocity data (>50% within 1 hour; 57% Faster Payments)	**[CREDIBLE]** CREDIBLE	Outseer/RUSI-based UK bank data (2024); specific sample of £7.2M over two months; methodology described in source publication	UK-specific dataset; Faster Payments is a UK-specific rail; velocity and channel mix may differ significantly in US, EU, and other jurisdictions with different payment infrastructure
BioCatch 2 million mule accounts figure	**[CREDIBLE]** CREDIBLE	BioCatch 2024 report; 257 institutions across 21 countries; BioCatch behavioral biometrics provides institutional-level account classification data	"Flagged" may reflect detection tool output rather than confirmed mule accounts; false positive rate not disclosed; figure may reflect detection capacity improvement as much as actual account inventory increase
Mule network cross-vertical function (serving ransomware, fraud, BEC simultaneously)	**[CREDIBLE]** CREDIBLE	KPMG "mule factory" documentation; consistent with academic and financial crime research on professional money laundering networks; TRM Labs outsourcing analysis consistent	Specific revenue attribution between cybercrime verticals is not documented; cross-vertical function is inferred from network-level analysis rather than confirmed case-level attribution
Group-IB UNC2891 Google Ads mule recruitment	**[CONFIRMED]** CONFIRMED	Group-IB published operational case study; specific TTPs documented including Google Ads and Telegram recruitment methods; consistent with KPMG and other independent sources	Case-specific; UNC2891 is one documented instance; prevalence of Google Ads recruitment across herder networks as a whole is not separately quantified

Rosfinmonitoring cooperation limitations	**[ANALYST INFERENCE]** ANALYST INFERENCE	Inferred from Russian state protection framework (Dark Covenant 3.0); historical pattern of selective Russian financial intelligence cooperation on cybercrime cases; no confirmed open-source case where Rosfinmonitoring actioned a ransomware-linked mule referral	Absence of confirmed cooperation cases does not prove non-cooperation; some bilateral cooperation may occur on non-ransomware financial crime cases that is not relevant to EDP scope

Intelligence Gaps

- Ransomware-specific mule flow attribution: The available dataset (BioCatch, UK bank data) covers all cybercrime mule flows, not ransomware-specific flows. Isolating the mule network capacity dedicated specifically to ransomware cash-out layering is not currently possible from open sources.
- Russian-based mule network operators: The herder and professional laundering crew tier serving RU-language ransomware groups is not publicly documented. Identifying these operators — and screening for FSB protection relationships before any attribution action — is the primary HUMINT requirement for this node.
- Integration-stage asset acquisition volumes: The total value of ransomware proceeds integrated via real estate, luxury goods, and front companies is not quantified in any available open source. This gap limits policy prioritization for integration-stage regulatory action.
- Mule network herder prosecution baseline: An accurate cross-FVEY baseline for herder-tier versus retail mule prosecution rates does not exist in publicly available statistics. Establishing this baseline is prerequisite to measuring whether disruption actions are reaching the right tier of the network.

SECTION 8: ANALYST ASSESSMENT

Key Takeaway

Mule networks are the final operational stage of the ransomware monetization chain and the most difficult node to fully disrupt because of the structural asymmetry between the account supply (nearly 2 million flagged accounts in 2024) and any realistic law enforcement interdiction capacity. Individual mule arrests and account freezes do not degrade network capacity at scale — the recruitment pipeline continuously replenishes the account supply. The strategic insight for Node 09 disruption is that the leverage point is not the accounts but the velocity: real-time payment rails are the operational enabler, and structural intervention at the payment network level is the only mechanism that can disrupt the layering function without depending on individual account identification.

Herder-tier prosecution remains the highest-value targeted action because it removes operational knowledge that individual accounts do not provide. The cross-vertical function of professional herder networks — simultaneously servicing ransomware, fraud, BEC, and other cybercrime cash-out — means that a single successful herder prosecution produces disruption value across the entire cybercrime ecosystem, not just the ransomware supply chain. This multiplier effect is the primary argument for dedicating HUMINT and financial intelligence resources to herder identification rather than accepting the current state of near-exclusive retail mule prosecution.

Priority Recommendation

Immediate: Reorient mule network disruption metrics from retail mule arrest counts to herder-tier prosecution rates. Current FVEY reporting on mule network enforcement emphasizes arrest totals and account freeze volumes — metrics that reflect operational activity but not strategic disruption. Establishing a cross-FVEY herder prosecution rate baseline and setting a measurable target for shifting the prosecution mix toward herder-tier actors is prerequisite to evaluating whether Node 09 disruption is producing durable ecosystem-level effects.

Near-term: Engage payment network operators (Pay.UK, The Clearing House, EBA Clearing) directly on real-time mule detection model development. The >50% fund-exit-within-one-hour velocity characteristic of mule

networks means that any detection mechanism operating on a next-day or end-of-day cycle is structurally ineffective. The UK APP fraud reimbursement liability framework — which creates a financial incentive for bank investment in real-time detection — is the regulatory model; equivalent frameworks in the US and EU would substantially expand the functional reach of payment-rail-level mule disruption.

Medium-term: Develop a cross-FVEY integration-stage regulatory action program targeting the primary integration vehicles (real estate, luxury goods, front companies). Integration-stage disruption does not require LE cooperation with Russia and is not constrained by the FSB protection framework — it operates in the jurisdictions where the assets are acquired. Beneficial ownership registry requirements and enhanced due diligence for cash transactions in real estate and luxury goods markets are viable regulatory actions that close the terminal stage of the laundering chain.

Sequencing note: Node 09 is a Phase C node. Its disruption value is contingent on the effectiveness of Phase A and B actions upstream. If OTC brokers (Node 01), exchanges (Node 02), and mixers (Node 08) are effectively disrupted, fewer funds reach the mule network pipeline and at lower "cleanliness" — increasing the compliance risk for every mule account that receives a transfer. Phase C mule actions are most effective when Phase A financial pressure has already reduced the volume and raised the risk profile of fiat entering the mule network.

Connection to EDP Disruption Playbook

Node 09 (Mule/Money Laundering Networks) is a Phase C node alongside Nodes 05 (Botnet/Loader Ecosystems) and 06 (Leak Site Hosting Stack). Phase C targets delivery and monetization — the operational outputs that convert ransomware capability into criminal profit. Node 09 represents the monetization side of Phase C: without functional mule networks, ransomware proceeds remain in cryptocurrency, subject to ongoing blockchain forensics and OFAC pressure. Mule network disruption is therefore the terminal-stage complement to the crypto-side financial actions in Phases A and B.

The Phase C sequencing is load-bearing for Node 09: Phase A and B actions that reduce the volume of fiat reaching mule networks compound the effectiveness of Phase C mule disruption. The full compound effect of the EDP playbook — financial pressure at every stage of the monetization chain — is most visible at Node 09 because it is the point where all upstream disruption actions manifest as reduced inflow volume, degraded "cleanliness" of received funds, and increased compliance risk per transaction.

Dependency Map Update Recommendations

Current Node 09 Field	Current Value	Proposed Change	Rationale
Replace Difficulty	MEDIUM	Sub-categorize: retail mule accounts = VERY LOW; structured herder networks = MEDIUM; professional laundering crews = HIGH	The aggregate MEDIUM rating obscures the actionable distinction. Retail accounts are nearly instantly replaceable (2 million active in 2024). Herder networks take months to replace. Professional crews take years. Disruption resource allocation should reflect this tier-specific profile.
Primary Owner	FVEY LE FOs + FNS referral + Rosfinmonitoring pipeline	Add payment network operators (Pay.UK, The Clearing House, EBA Clearing) as co-primary for real-time rail disruption; de-emphasize Rosfinmonitoring pipeline as operationally limited for ransomware-linked flows	Payment network operators have structural leverage over the velocity advantage that makes mule networks operationally effective. Rosfinmonitoring cooperation is a formal channel but structurally limited for ransomware cases per Dark Covenant 3.0 framework.
No integration-stage node or sub-node	N/A	Recommend adding an integration-stage sub-node or supplementary tracking layer under Node 09 covering real	The integration stage is the terminal point of the laundering chain and the only stage where disruption does not depend on blockchain forensics, LE

		estate, luxury goods, and front company integration vehicles	cooperation with Russia, or real-time detection. Dedicated tracking enables regulatory action prioritization without the constraints affecting upstream nodes.
No cross-vertical disruption multiplier noted	N/A	Add a note to Node 09 that herder network disruption has cross-vertical effect across ransomware, fraud, BEC, and carding cash-out; flag this as the primary argument for prioritizing herder prosecution in interagency resource allocation	The cross-vertical function of professional mule networks is a structural feature that multiplies the disruption value of herder-tier prosecution above its ransomware-specific contribution. This is a concrete argument for FVEY resource investment that is not reflected in the current node description.

Follow-On Research

- Establish cross-FVEY herder prosecution rate baseline: compile national prosecutorial statistics to determine current herder-tier versus retail mule prosecution mix; set measurable target for shifting the mix toward herder-tier actions.
- Identify Russian-based herder and professional laundering crew operators serving RU-language ransomware groups: HUMINT and financial intelligence priority; Dark Covenant 3.0 screening required before any attribution action.
- Model payment network operator intervention points for real-time mule detection: engage Pay.UK, The Clearing House, and EBA Clearing on technical feasibility of network-level real-time mule classification models; assess APP fraud liability framework replication in US and EU jurisdictions.
- Quantify integration-stage ransomware proceeds: commission or task financial intelligence analysis to estimate the total value of ransomware proceeds integrated via real estate, luxury goods, and front companies in FVEY jurisdictions annually — prerequisite for integration-stage regulatory action prioritization.
- Assess Rosfinmonitoring pipeline utility: conduct a structured review of any historical cases where Rosfinmonitoring acted on ransomware-linked financial intelligence referrals; determine whether a residual cooperation pathway exists and under what conditions it is actionable.