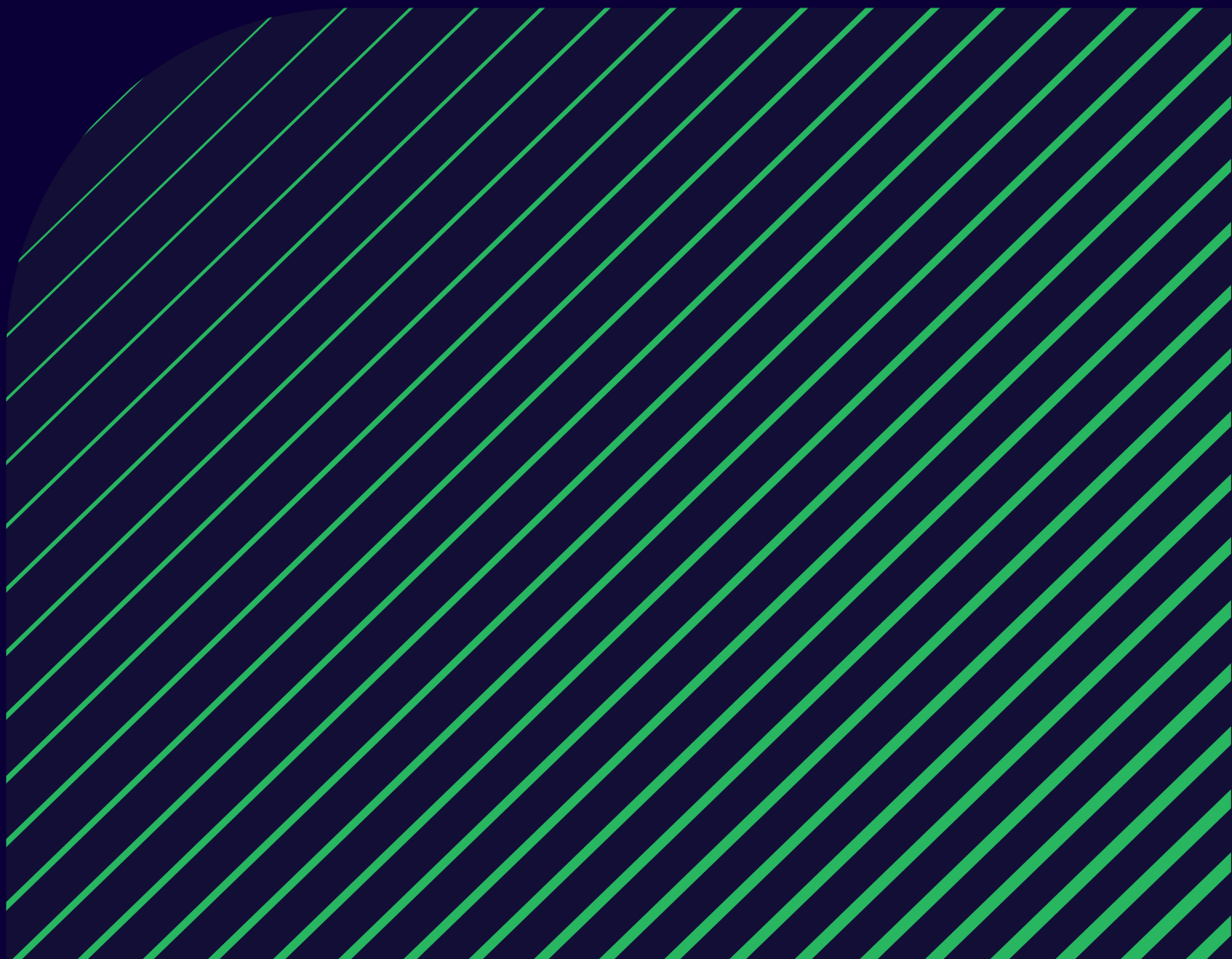
SYNECTICS SOLUTIONS

A realistic blueprint to start and scale ongoing AML screening

Detect mules earlier and faster, without the operational overwhelm.



Preface

The UK's money muling threat has reached previously unseen levels and is now considered a standalone strategic priority by regulators and banking leaders alike. This shift is driven by three converging factors.

Social media connects laundering recruiters to a conveyor belt of new mules – some unwitting, others willing. Digital banking has changed behaviours so much that genuine customers now often look like criminals. **And, perhaps most importantly, money launderers are now seriously hindered by point of application controls.**

In the last 5 years*, checks using the National SIRA fraud risk intelligence consortium have prevented approximately 689,000 fraudulent applications.

Unable to meet laundering demand through new accounts alone, organised gangs are targeting existing customers.

They're harvesting safely-boarded accounts, then timing transaction activity around fixed screening schedules and in many cases, busting out shortly thereafter. This all means that periodic checks are no longer enough to protect banks and their customers from money laundering.

- Checks must now happen post-application – becoming a continuous process whereby new risk signals are flagged immediately throughout the customer lifecycle.
- When shared between institutions, these signals can also enrich point of application checks – arming teams with a fuller picture of an applicant's future laundering risk.

AML and risk leaders recognise the case for perpetual screening. What slows progress is the scale of the shift: securing board approval, managing referral flow, or planning back-book remediation can feel overwhelming.

This blueprint acts as a guide to kickstarting a sustainable mule detection strategy. It breaks the challenge into tested, realistic steps - showing how to start small, prove value, and scale over time while staying firmly aligned with compliance expectations.

*Time period data is held for in National SIRA, owned and operated by Synectics Solutions.

The perfect conditions for a money muling wave

Muling activity continues to surge among “traditional” student-aged recruits and the over 40s.

- **Easy mule recruitment:**
  By exploiting social media, WhatsApp and even AI-generated job adverts, herders can easily profile, contact and recruit a theoretically endless supply of mules.

- **The cost-of-living crisis:**
  It’s true that fraud and other financial crimes increase during times of economic hardship. Mule herders know that targets may be more vulnerable to the lure of cash.

- **Smaller, less “serious” transactions:**
  Narrative economics play a role here. Mules rationalise laundering when amounts are low (e.g. £50 vs £1,000), telling themselves a story that it’s not a “real” crime. This cognitive dissonance makes low-value fraud feel more acceptable.

- **Social engineering skills:**
  OCGs are strategists and psychologists, and place mules exactly where they want them. Mule herders may use social engineering to trick first-time mules, or persuade previous contacts to engage in riskier transactions.

- **Low-friction processes:**
  Shorter timelines for everything from onboarding to sending money don’t leave much time to fact-check and reflect. Muling is often a tap-and-done job.

Mules and the criminal gangs behind them will adapt to any new AML control banks put in place.

But the preference for scattered, low-value activity — using consumers as human shields — isn’t going anywhere. The risk to reward trade-off is just too good.

This comes at a time when regulators are reframing money muling not as clear-cut crime, but the potential exploitation of vulnerable people. A distinction that carries weight under Consumer Duty and further complicates questions around friction levels.

A look inside the modern money mule economy

To uncover the true scale of the money muling threat, we worked with Tier 1 banks to interrogate their back-books for hidden money laundering links.

We screened their highest risk customer segments against our National SIRA shared fraud risk intelligence database. National SIRA is the largest consortium of its kind, spanning multiple sectors and containing confirmed, suspected and clear fraud data.

The results

Our original research uncovered that 75% of money mules evade early detection.

We defined "early detection" as the typical point of application and post-onboarding checks used by Tier 1 Banks. The fact that so few money muling signals exist at application stage is strong evidence that launderers have carefully studied – and are successfully bypassing – periodic rescreen schedules.

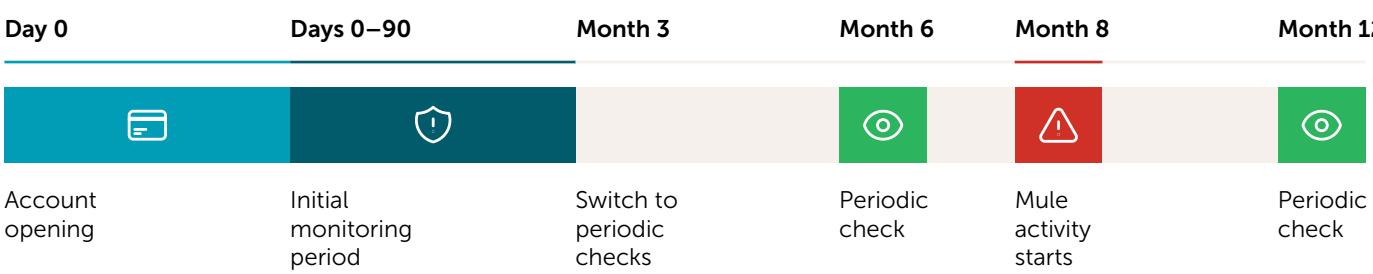
Our analysis also revealed a previously undocumented pattern in mule behaviour: a distinct 'time to mule'.

Accounts appear dormant and risk-free for several months after onboarding, only to enter a high-intensity laundering phase across multiple institutions in rapid succession. Because these mules operate through fully verified accounts and identities, they slip through conventional controls.

Here, we see mules exploiting systemic blind spots in typical periodic monitoring strategies. As a result, compliance is compromised across the Money Laundering Regulations, Consumer Duty, and even the PSR's APP scam rules. It's clear that continuous AML screening is the only credible way to catch the majority of mules given current behavioural trends.

Our hidden mule risk research findings

- The median time for an account to engage in mule activity is 8 months. During this period, would-be mule accounts maintain a façade of normality.
- Mules offend on average across 3.6 banking organisations. Once they begin offending, the time frame between incidents is approximately 2 weeks.
- Due to a long dormancy period, 75% of mule accounts would be missed by standard point of application screening and typical post-onboarding, periodic checks.
- Mules are associated with fraudulent and innocent accounts – helping to cover their tracks and blend into the crowd.



Your blueprint for kickstarting ongoing AML screening, tested with tier 1 banks

The following guidance is designed with practicality in mind. It focuses on manageable actions almost every banking leader can take to kickstart ongoing mule screening, while maintaining strong evidence of compliance.

Screening your back-book

We'll address it head-on. To manage the mule threat and continue being compliant, you will need to screen your entire back-book at some point. But what you don't need is a complete and functioning ongoing AML screening strategy from day one.

With a phased approach to back-book screening – whereby your highest risk segments take priority – you can make confident, credible progress. Controlling active threats from laundering without hitting your team with millions of referrals at once.

Every strategy will be different. But here's a theoretical example:

Smart Bank has 10 million customers to screen. To get started, they pass a batch of their highest risk customers to an ongoing screening provider, who checks against syndicated risk intelligence. The high-risk batch is "washed" against the data, and categorised into:

- **High risk**
  Immediate review and ranked by severity.
- **Medium risk**
  More frequent checks, with high risk rules applied at the next screening.
- **Low risk**
  Lighter-touch screening. We chose 180 days.

Working with the resource available, Smart Bank starts at the top of the risk list and works down. This is step one of a larger plan to screen their entire back-book. In the meantime, they can rest assured that the highest AML and compliance risk is under control, and start learning from their continuous intelligence.

Crafting your mule rules

AML and counter-fraud teams walk a fine line: protecting consumers while clamping down on laundering.

That balance is perhaps hardest in mule detection. Modern behaviour, such as having multiple accounts, making sporadic payments and gig-economy income, often looks suspicious while being perfectly safe.

We've met (and helped) many companies who've mis-identified and paid the price in referral spikes, poor customer service and stunted growth. From testing with Tier 1 banks, we've found 3 distinct differences between rules that create false positives and operational friction and those that deliver effective mule detection.

01 Check in with your baked-in biases

Some signals will always be clear red flags, like smurfing, roundtrips and geographic anomalies. However, the rapid changes in mule tactics and banking behaviours mean that even recently calibrated rules could be unknowingly biased toward atypical – and innocent – customers.

To mitigate the risk of bias resulting in poor decisions, we tested the following:

- **Attribute weighting in overall mule risk scoring:** For example, are peaks and troughs in transaction activity pushing an account into a high-risk cohort, despite such activity being relatively low-risk amongst today's typical customer?
- **What counts as a deviation for the individual vs. their peer group.** I.e., the nature of payments for gig-economy workers. Late night, high-velocity payments into digital wallets, for example.
- **Behaviours in borderline cohorts.** In some cases, we ran a data wash of moderate-risk accounts to see whether behaviours flagged were truly anomalous. Where resources allow, this sense-check helps to avoid over-penalising emerging or unfamiliar customer segments.

02 Balance detection with prediction

Once appetite is clear, align rules with how mules actually behave. A practical start is to enrich your AML sets with specialist "mule rules".

These mule rules, informed by confirmed laundering cases in shared intelligence databases, are designed to detect early behavioural signals – the subtle markers that appear before an illicit transaction. Such insight enables you to better control risk by:

- Flagging accounts with a high likelihood of becoming mules - at application stage and throughout the customer lifecycle.
- Applying proportionate friction, from enhanced checks to proactive AML/pKYC measures.
- Declining applications outright where risk exceeds appetite.
- Protecting genuine customers by distinguishing modern usage patterns from bad actors.

03 Roll out realistically

A strong strategy needs realistic deployment. Use your back-book data wash as the staging ground:

- Apply full, enriched mule rules to high-risk accounts immediately.
- Apply lighter rules to lower-risk cohorts until resources expand.

A credible platform will facilitate multiple rule sets on different cycles, so higher-risk accounts get closer scrutiny while lower-risk accounts are still screened in a compliant, manageable way.

Getting budget buy-in

Securing budget is easiest when losses are visible and recurring - something leaders modernising mule detection strategies know all too well.

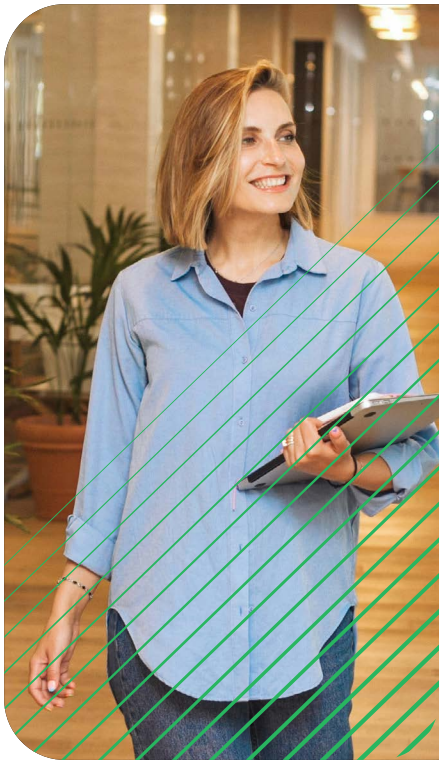
Non-compliance fines remain a major risk, but regulatory guidance is broad and open to interpretation. What one board sees as proactive ongoing screening, another may judge as insufficient. Perpetual AML screening also drives more referrals and reporting, complicating the investment case.

Even so, the rationale for action is clear.

Scattered mule activity, rising illicit transactions and unpredictable customer behaviours mean that even basic AML and KYC compliance now demands continuous monitoring, post-application.

Regulators increasingly treat mule activity as a strategic risk in its own right - not just a fraud by-product - and the cost of failing to address it is high. The UK's new Failure to Prevent Fraud offence reinforces this, obliging firms to evidence 'reasonable procedures' to prevent fraud by associated persons as part of their compliance posture. While not explicitly focused on mule activity, such risks may be considered within a broader fraud risk assessment.

Beyond fines, fraud and risk leaders face wasted onboarding effort, forced account closures, lost investigation hours and reputational damage. But perhaps most importantly, they impact business growth. As protections for unwitting mules become integral to Consumer Duty, customers will increasingly factor scam safety into their decision-making hierarchy.



Your budget case: efficiency meets inevitability

01 Frame the ROI in terms of prevention

Every mule account closed represents sunk cost in onboarding, servicing, and investigation. Ask:

- What if that account had been flagged earlier?
- How many new customers must be boarded to replace the value lost to just one mule?
- How much transaction monitoring spend could be avoided if even 10% of flagged transactions were prevented at the source?

02 Choose automation that extends beyond detection

A credible mule strategy needs automation not just for data screening but for downstream case management and lower-stakes customer decisions. Make clear that without extended automation, complexity will outstrip human capacity, and budgets will suffer under the weight of manual process.

03 Start with the back-book, but don't wait for perfection:

Your back-book is the single richest source of laundering signals. Use it to evidence where exposure is greatest and to train future-facing controls. Launch with it, knowing you'll refine as typologies evolve. Perfection is neither possible nor required to demonstrate immediate value.

Summary

Ongoing AML screening leaves launderers with far fewer places to hide. It flushes them out of supposedly safe havens like boarded accounts. It separates genuine customer behaviour from criminal camouflage. And it gives you the foresight to say no upfront, easing transaction fraud pressures.

As perpetual strategies mature and align across banks, the balance of power will shift away from OCGs gaming the system and back towards AML teams. But with mule tactics evolving fast and regulators issuing headline penalties in 2025, change today matters most.

This blueprint shows that while transitioning to continuous screening is challenging, it isn't insurmountable. Even with millions of back-book customers, limited mule-specific rules, or a finite budget, the interim steps here are accessible to almost every AML and counter-fraud team. Enabling progress, if not perfection, from day one.

As one fraud leader put it:

"The list is only ever getting longer - we might as well get stuck in."

Liese Rushton
Fraud Strategy Consultant & AML Specialist

More information:

info@synectics-solutions.com
+44 (0) 333 234 3409
synectics-solutions.com

SYNECTICS
SOLUTIONS