

Scams Don't Start at Payment. Neither Should Your Defense.

Six pillars for building a
cross-platform, intelligence-driven
approach to customer protection
in the new liability era

Get Started



LexisNexis
RISK SOLUTIONS



Scammers operate as connected networks. Many banks still defend as disconnected teams.

> Most scam journeys begin outside the bank, long before the payment event. Criminals operate across platforms, channels, devices and networks, and only a fully connected, intelligence-driven bank can defend effectively.

This whitepaper outlines why scams must be treated as ecosystems, how regulation is shifting toward that model, and what a modern, connected scam strategy looks like in practice. It introduces six core pillars to help banks intervene earlier, reduce customer harm and meet evolving global expectations.

Contents

The full scam ecosystem

Scams begin long before the first transfer	3
Exploiting fragmented bank controls	4
The global liability shift	5
Regulatory direction evolves	8

Six pillars of a connected scam strategy

Strategic overview	9
• Unified customer view	10
• Global digital identity	11
• Customer intelligence	12
• AI-driven assessment	13
• Connected mule strategy	16
• Ecosystem partnerships	17

Conclusion

An operating model that makes it all work	18
A connected defense for an ever-evolving threat	19

Scams begin long before the first transfer

- > Scammers typically reach victims through scalable, high-trust channels such as social media, messaging apps, spoofed calls, phishing, job boards and online marketplaces.

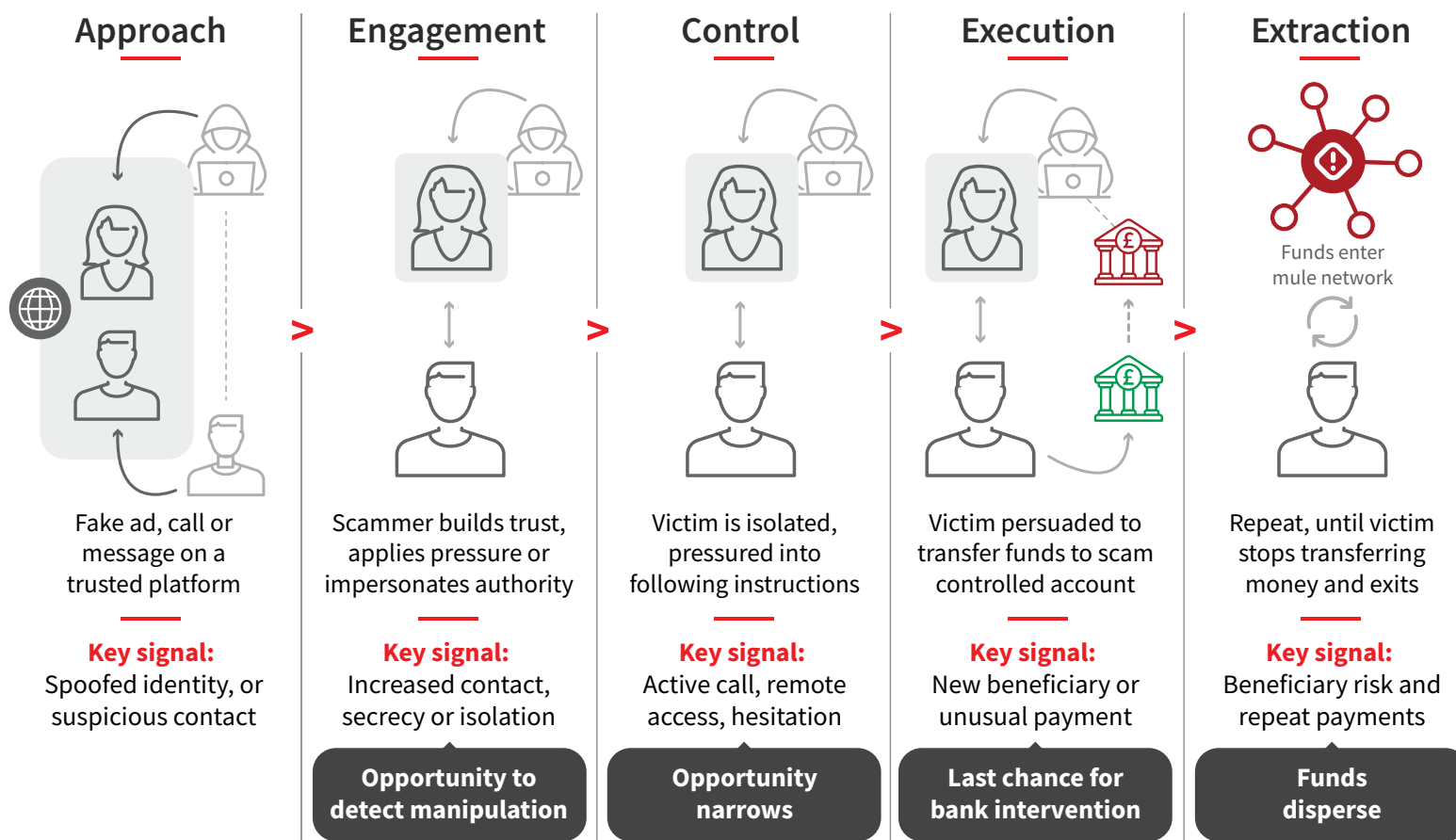
The goal is not just initial contact, it's control. Victims are guided into a controlled journey where criminals set the narrative, isolate them from advice and pressure them into transferring funds to mule accounts.

To maintain control, scammers combine technical tools and psychological manipulation, including:

- Remote access and screen-sharing
- Spoofed identities and fake environments
- Scripted coaching for bank-customer interactions
- Urgency, fear and emotional pressure

This control persists until funds are moved and often continues across repeat payments in longer scams like investment or romance fraud.

A Scam Isn't A Payment Event — It's A Long Customer Journey



Exploiting fragmented bank controls

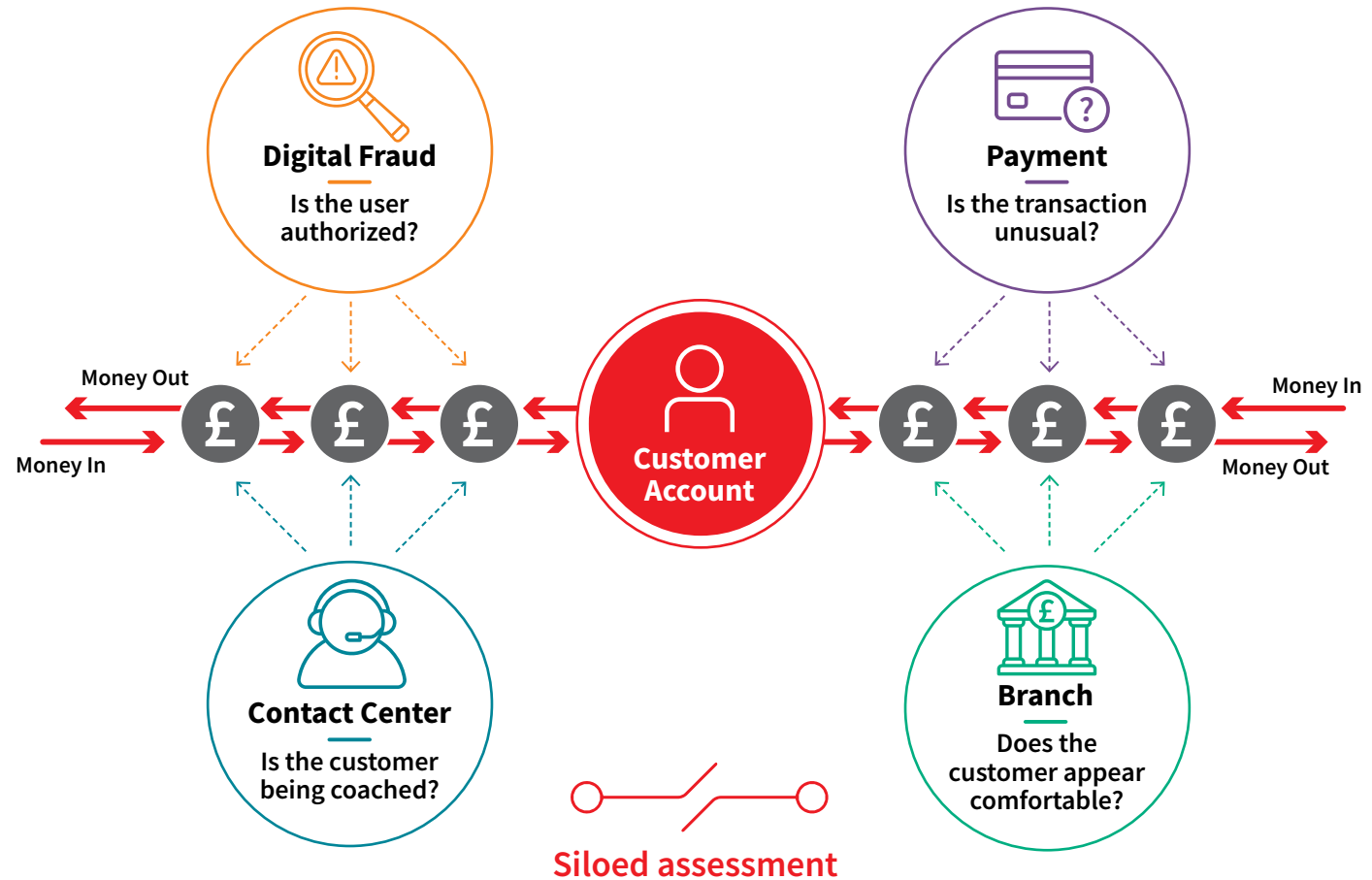
> By the time a payment is initiated, the scam is often already entrenched. Yet many banks still rely on siloed controls split across channels, payment types and teams.

Common gaps include:

- Disconnected digital, branch and call center views
- Inbound and outbound payments assessed separately
- Device and behavioral signals trapped within channels
- Inconsistent visibility across payment schemes
- Fragmented tools and data across teams

Scammers operate as networks. Banks often operate in silos. That mismatch is where scams succeed, and why regulatory pressure is increasing.

Inadequate Defense: A Fragmented Response To An Organized Threat



When bank defenses don't communicate and share knowledge, it gives organized scammers an advantage.

The global liability shift: Why siloed controls can no longer survive

LIABILITY FOR SCAMS IS EXPANDING...BUT PROGRESS VARIES BY COUNTRY.



United Kingdom

Mandatory reimbursement for most APP scams



Singapore

Established shared accountability and earlier intervention



Australia

Cross-sector scam prevention framework entering implementation



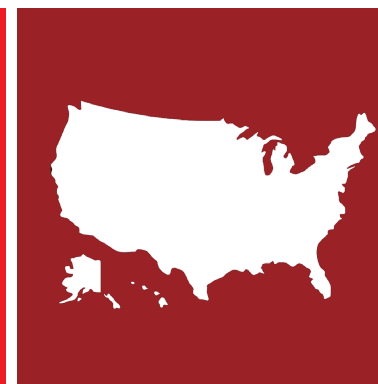
European Union

Stronger obligations to prevent fraud and customer manipulation



India

Developing targeted digital-fraud compensation



United States

Emerging pressure: Stronger prevention expectations

MORE SHARED SCAM LIABILITY

LESS SHARED SCAM LIABILITY

Banks are facing greater responsibility for preventing scams earlier, sharing intelligence and protecting customers across the full scam journey.

Around the world, policy direction is converging: Scam prevention must be proactive, cross-channel and network-aware, with clearer accountability for outcomes.



United Kingdom

Mandatory reimbursement for most APP scams

- > The UK has one of the most mature scam liability regimes. It requires mandatory reimbursement for most authorized push payment scams and introduces a 50/50 cost split between sending and receiving payment service providers.

That structure forces banks to care not only about the customer initiating a payment, but also the destination, the beneficiary risk and the network patterns around mule activity. It also hardens the expectation of contextual, early intervention and consistent cross-channel controls, because a bank cannot credibly demonstrate reasonable steps if one channel protects customers and another channel is effectively blind.



Singapore

Established shared accountability and earlier intervention

- > Singapore established shared accountability through its Shared Responsibility Framework, in effect since 12.16.24. This defines specific anti-phishing duties for financial institutions and telcos and sets expectations for reimbursement where those duties are breached.

The framework uses a waterfall approach, with responsibility considered first for the financial institution and then for the telecommunications company. This strengthens consumer protection while encouraging earlier intervention and clearer accountability across the wider scam ecosystem.



Australia

Cross-sector scam prevention framework entering implementation

- > Australia has established a cross-sector Scams Prevention Framework covering regulated services provided by banks, telcos and digital platforms. This will require regulated organisations to prevent, detect, disrupt, report and respond to scams.

Relevant organisations must become members of the Australian Financial Complaints Authority from 09.01.26; most substantive obligations will apply from 03.31.27. The framework formally recognises that effective scam prevention requires coordinated action across the wider ecosystem, rather than action by banks alone.

PROOF POINT

A Tier-1 UK Bank Mitigates More Scam Losses By Using Beneficiary Intelligence

Challenge: The bank needed to protect customers from authorized push payment scams as reimbursement expectations tightened.

What changed: Deployment of scam and beneficiary intelligence models to widen detection beyond the payer, without increasing alert volumes.

Results: A **366%** increase in scam value protected in six months and **275%** more scams detected at the same review rate.



European Union

Stronger obligations to prevent fraud and customer manipulation

- > The EU's agreed Payment Services Directive 3 and Payment Services Regulation reforms significantly strengthen expectations for fraud prevention and consumer protection. Measures include improved verification of payee, greater fraud-data sharing between payment service providers and stronger protections for impersonation-fraud victims.

Payment providers will be expected to identify risk and intervene earlier, rather than relying primarily on controls at the point of payment. This increases the need for connected intelligence across customer behaviour, identity, beneficiaries and payment activity, as fragmented controls may identify only one part of a scam. These reforms will apply following final adoption and the relevant implementation periods.



India

Developing targeted digital fraud compensation

- > India is moving toward more structured protection for victims of digital-payment fraud. During 2026, a targeted compensation framework for qualifying small-value digital-fraud losses was reported, marking further progress from earlier proposals to strengthen compensation and consumer redress.

The developing approach remains more limited than the broad mandatory APP reimbursement framework operating in the UK. India should therefore be viewed as a market strengthening targeted consumer protection, rather than one with a comprehensive scam-reimbursement regime already in place.



United States

Emerging pressure: Stronger prevention expectations

- > The US remains broadly enforcement-led for many authorized scam scenarios, but the scale of loss is creating sustained pressure for stronger prevention and clearer accountability.

Reported fraud and internet crime losses continue to show that the scam problem is now too large, too behavioral and too networked for warning-only or channel-specific controls to materially reduce harm.

Whether reimbursement is mandated today or not, expectations are shifting toward demonstrable prevention before the money moves.

India shows a market transitioning toward stronger expectations through:

- Proposals to unify and strengthen compensation and redress frameworks
- Growing public expectation that banks should reimburse scam victims
- Increased scrutiny of digital fraud volumes
- Isolated court rulings ordering refunds on a case-by-case basis
- Improvements in authentication, risk scoring and fraud controls under review

India remains a watch-this-space market: signaling movement toward greater consumer protection, but without a defined, systemic scam-liability regime in place.

Regulatory direction evolves

> Regulators worldwide are tightening expectations on scam prevention. While approaches vary, the global trajectory is clear.

- Banks must adopt holistic, cross-channel, behavioral and networked defenses
- Siloed controls are becoming increasingly misaligned with regulatory expectations
- Customer protection must be proactive
- Detection must start before payment
- Banks must demonstrate end-to-end cross-channel prevention



A fully connected scam strategy: Six core pillars

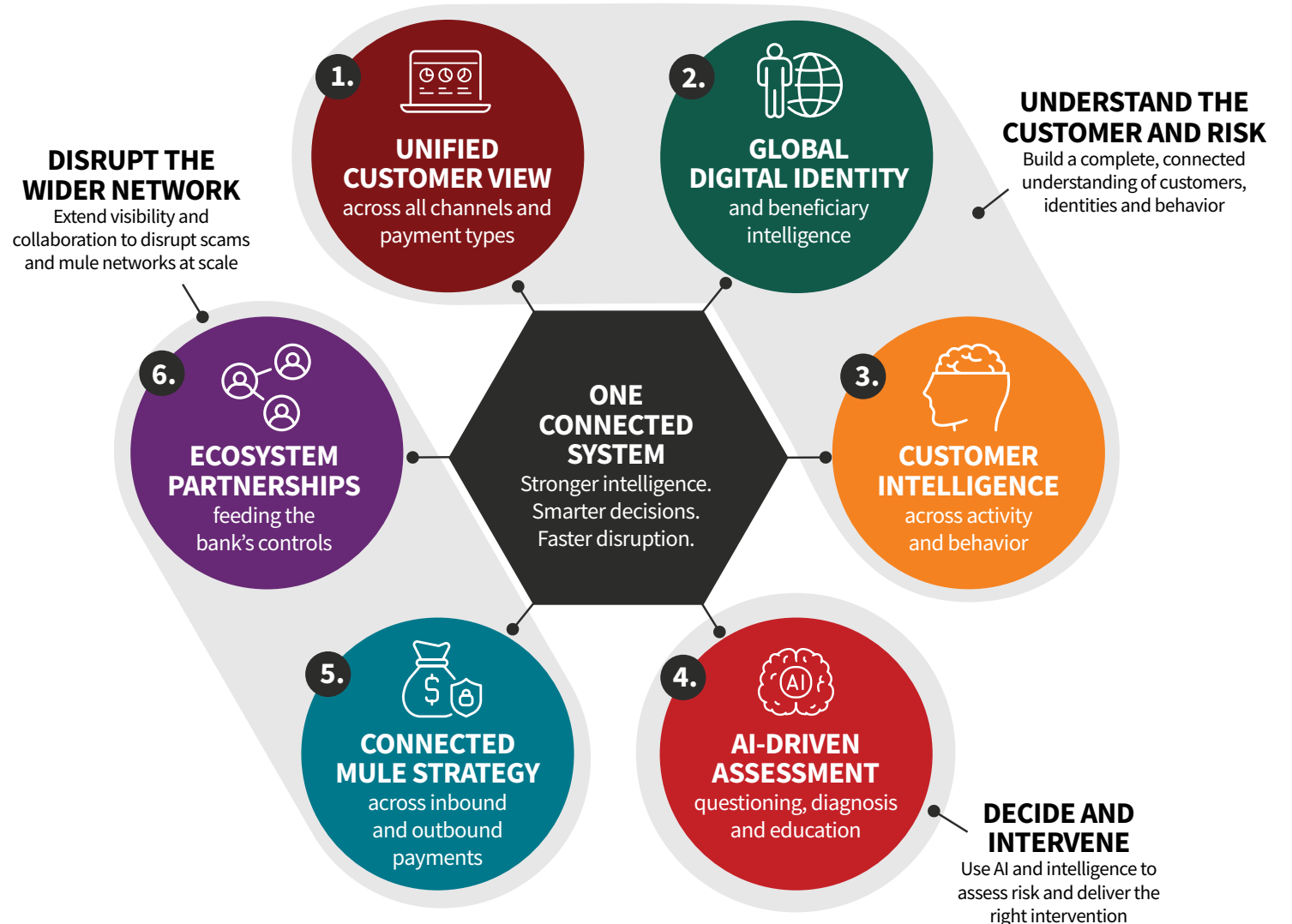
> **Effective scam prevention requires a connected approach that detects manipulation, understands intent and disrupts networks across the full lifecycle.**

These six strategic pillars work together as a single system, closing the structural gaps criminals exploit, strengthening intelligence flow across the organisation and enabling earlier, more consistent and more effective intervention.

We'll go into each in detail on the following pages.

Six Core Pillars of a Connected Scam Strategy

One connected system that strengthens itself through shared feedback, intelligence and cooperation





Scam Strategy Pillar 1

Unified customer view across all channels and payment types

- > **Scam detection collapses when channels do not share intelligence. A connected bank requires one risk identity per customer and one behavioral timeline that persists across the journey, not just within a single channel.**

It also needs one intelligence layer shared across digital, branch, telephony and card channels, so scam insight is not trapped with whichever team saw it first.

At the point of decisioning, this must translate into one decision engine across Faster Payments, CHAPS, card payments and international payments, with scam-type models applied consistently across use cases such as purchase, impersonation, romance and investment scams.

Without this, scammers will exploit blind spots and quickly adapt their strategy. A fragmented bank cannot realistically move as quickly as a fraudster operating across multiple platforms.



Key requirements for a unified customer view:

- One risk identity per customer
- One behavioral timeline
- One intelligence layer shared across channels
- One decision engine across payment types
- Scam-type models applied consistently across purchase, impersonation, romance and investment scams



Scam Strategy Pillar 2

Global digital identity and beneficiary intelligence

- > **Scammers work across many banks, devices, IP addresses, countries, channels, crypto platforms and mule networks. Banks need access to the same cross-industry visibility, because criminals reuse infrastructure and patterns across victims and institutions.**

LexisNexis® Digital Identity Network® provides device reputation, active call detection, email and IP intelligence, digital consortium insights, cross-bank beneficiary risk assessment, network link analysis, multi-channel behavioral patterns and crypto or gambling risk indicators.

The key requirement is operational. This intelligence must be consumed everywhere in the bank, not held in a single team or applied in only one channel.

PROOF POINT

A Layered Approach To Combining Data Sources Yields Success

A Tier One bank used device and transaction intelligence from LexisNexis® Digital Identity Network® to help identify links between devices, email addresses and phone numbers indicative of fraudulent activity.

Result: They achieved a **100%** increase in mule detection rates in one month and detected **\$469K** in fraud value.



Scam Strategy Pillar 3

Customer intelligence across activity and behavior

- > **Customer, device, global and behavioral analytics are now central to scam prevention because they capture manipulation signals that traditional transaction monitoring can miss.**

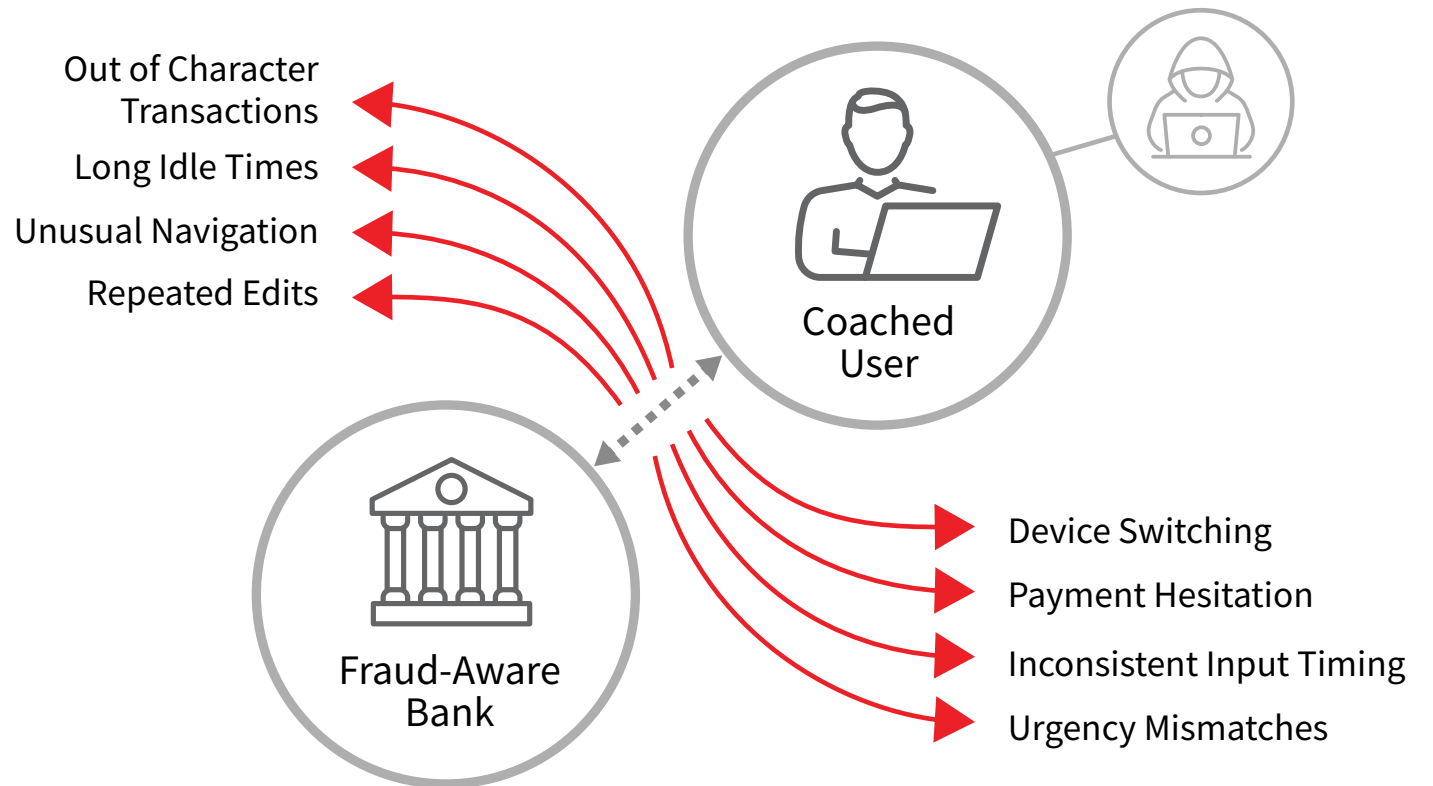
Remote-access behavioral signals go further. These may include cursor hesitation, operating-system anomalies, unnatural mouse movements, long pauses while waiting for instruction, repeated window switching, copy-and-paste behavior and coached navigation patterns.

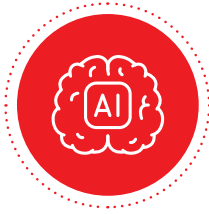
These signals often appear before the payment is completed, making them prevention-grade signals rather than purely investigative artifacts.

The decisive point is cross-channel unification. Behavioral intelligence must follow the customer across app, web and payment journeys. Behavior tells the story that siloed controls cannot.

Behavior can reveal manipulation before money moves

Examples of behavioral signals that help indicate coaching, pressure or forced urgency





Scam Strategy Pillar 4

AI-driven assessment,
diagnosis and education

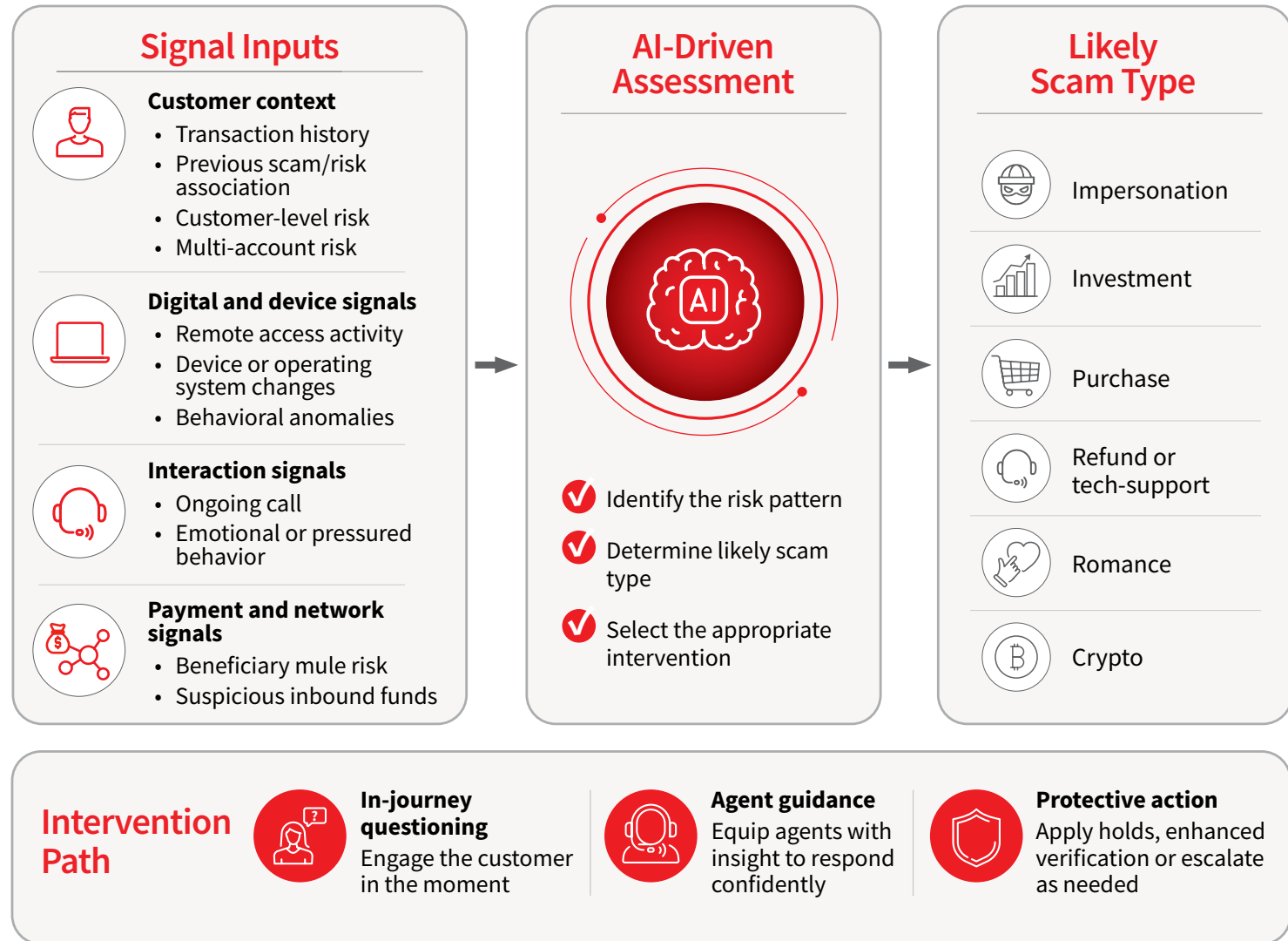
> There are three steps to AI-driven assessment. The first is scam detection.

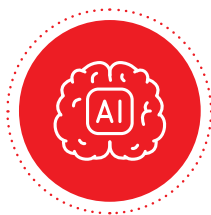
Prevention becomes real the moment the bank interrupts manipulation using the data it already has. By connecting customer, device, interaction and payment signals, the bank can detect pressure and deception as they emerge.

This approach disrupts coercive control, restores the customer's independent judgement and ensures the right safeguarding response is taken—through in-journey questioning, agent guidance, protective holds, enhanced verification or escalation when needed.



Step 1: Detection





Scam Strategy Pillar 4

AI-driven assessment,
diagnosis and education

> The second step: Targeted diagnosis.

AI-driven diagnosis can ask targeted, scam-specific questions in-journey or support a human agent working the alert.

These questions should analyze data to understand the reason for a transaction, validate the customer's experience and (in the next step) educate in a way that enables self-realization.



Targeted Diagnosis



Impersonation

- “Have you been instructed to make a payment today?”
- “Has anyone told you your money is at risk?”



Investment

- “Did someone contact you about this investment?”
- “Have you been promised guaranteed returns?”



Refund or tech-support

- “Has anyone told you they sent money by mistake?”
- “Did anyone ask you to download remote-access software?”



Romance

- “Is this payment for someone you have not met in person?”
- “Has the person encouraged secrecy?”



Purchase

- “Do you trust the site or seller you are buying from?”
- “Were you asked to pay outside the usual platform/process?”

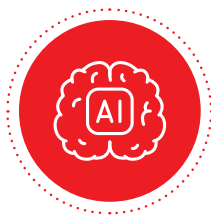


Crypto

- “Did someone instruct you to buy or move cryptocurrency today?”



Structured prompts challenge the scam narrative and support self-realization.



Scam Strategy Pillar 4

AI-driven assessment,
diagnosis and education

> The final step: Contextual education for the consumer.

Contextual education challenges the scam narrative, helps customers recognize the experience they are in and supports the right intervention.

Education should mirror common scam narratives. Romance, impersonation, investment and refund scams feel different emotionally and behaviorally.



Contextual Education



“Were you on a call today?” (Scammers often stay connected during payments.)



“Were you asked to install remote-access tools?”



“Would a legitimate organization request secrecy?”



“Does anything feel rushed or pressured?”



Diagnosis and education help the bank surface doubt, interrupt manipulation and guide safer customer decisions **before money moves.**



What This Enables



Recognize the experience



Restore independent judgement



Support the right intervention

> In-journey messaging, agent guidance, enhanced verification, protective holds or escalation.



Scam Strategy Pillar 5

Connected mule strategy across inbound and outbound payments

> Scams and mule networks are inseparable, and disrupting fund movement is as critical as stopping the initial payment.

A modern strategy requires:

- Inbound and outbound detection
- Risk propagation across transactions
- Multi-hop tracing
- Real-time intervention and recovery
- Cross-bank collaboration

PROOF POINT

Minimal Signals, Measurable Impact and Outbound Mule Detection... Without Inbound-Credit Data

A Tier-1 bank used networked digital identity intelligence to detect and disrupt outbound money-mule activity while maintaining low friction across mobile-app journeys.

Challenge: The bank needed to intercept outbound mule payments without introducing friction into everyday mobile-app journeys. The evaluation deliberately ran on a minimal signal set: mobile app only, with no web channel, no device profiling and no inbound credit feed, while keeping alert volumes low for manageable review.

What changed:

- The bank built a focused mule-detection model using LexisNexis® ThreatMetrix® on mobile-app payments and customer-history data, then layered in Digital Identity Network® intelligence to improve precision without adding friction.
- With no inbound-credit feed, network insight at the time of send was used to estimate recent-credit proximity. Approximately 60% of outbound mule events showed a same-week credit.

Results: **£4.4 million** estimated annual fraud savings, **93%** fewer false positives versus baseline, and **1,782%** increase in mule value captured.



Scam Strategy Pillar 6

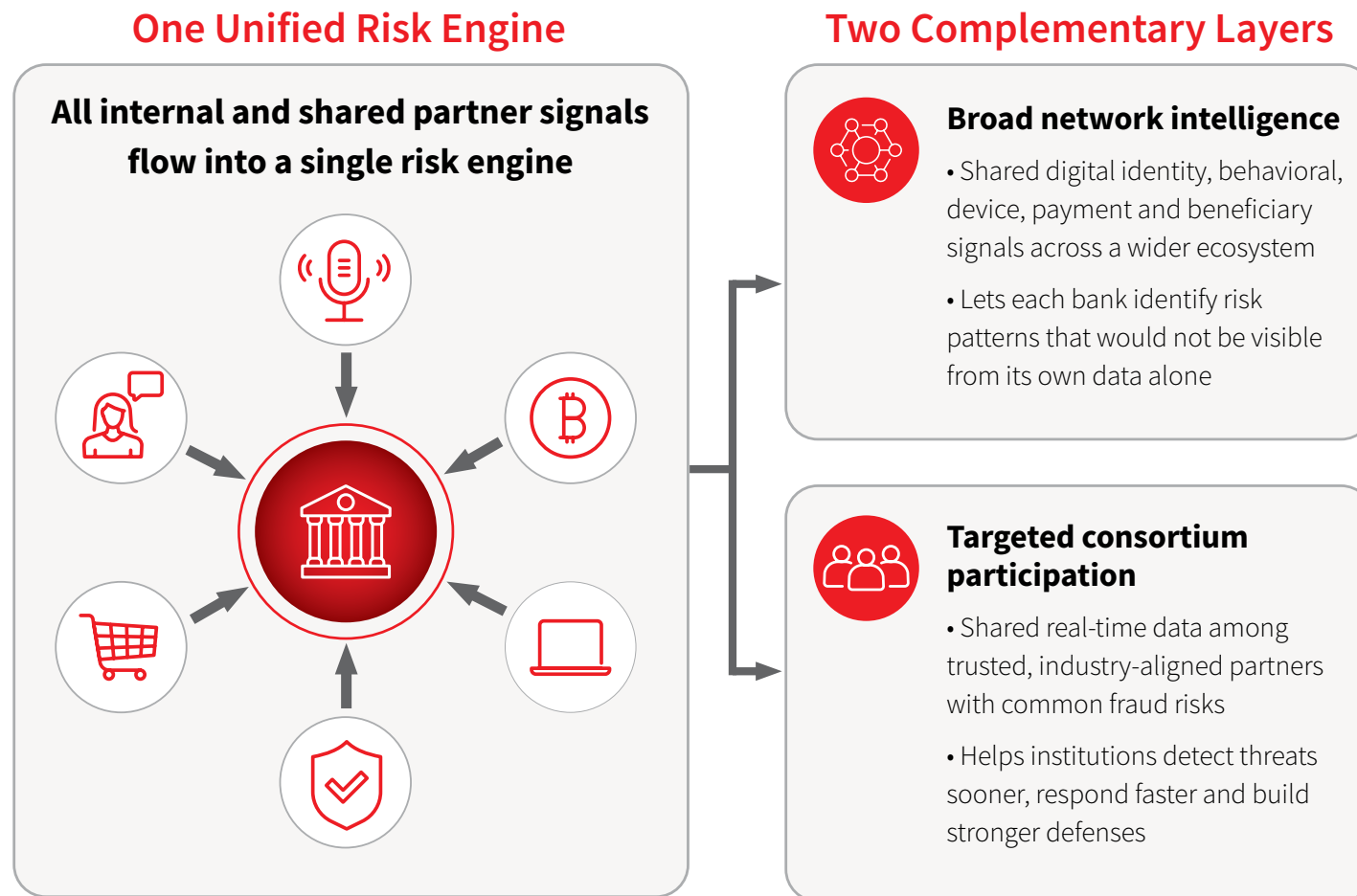
Ecosystem partnerships feeding the bank's controls

> Banks cannot see the full scam journey alone.

- Telecoms may see spoofing and call patterns.
- Social platforms may see fraudulent advertisements and fake accounts.
- Crypto providers may see laundering flows.
- Ecommerce merchants may see fraudulent purchases
- Remote-access tool vendors may see suspicious usage patterns.
- Regulators and law enforcement may see network-level intelligence.

Uniting these data sources requires operational integration. This data must feed into one unified risk engine, not sit separately by channel, function or partner type, so decisions are consistent, timely and defensible.

There are two complementary layers to this ecosystem approach. **Broad network intelligence** gives banks wider visibility, and **targeted consortium participation** enables more precise sharing and action. Together, they move defense from institution-level to ecosystem-level.



An operating model that makes it all work



The direction of regulation and global momentum is clear: Liability is shifting and expectations are tightening.

Payment Services Directive 3, the UK Payment Systems Regulator authorized push payment reimbursement model, Australia's Scams Prevention Framework, Singapore's shared accountability direction and wider global momentum all point toward the same conclusion: Regulators increasingly expect behavioral and network-aware controls. Banks must detect manipulation, not just fraud. Controls must be connected across channels, and prevention must happen earlier in the scam journey.

Institutions must also be able to demonstrate reasonable steps. That cannot be credibly shown through fragmented systems that only cover part of the journey. Siloed controls cannot meet modern expectations because they cannot see the whole journey, cannot intervene consistently and cannot explain outcomes in a way that stands up to regulatory scrutiny.



A connected strategy cannot be delivered by technology alone. It requires an operating model that matches the nature of the threat.

Unified governance is needed so scam prevention is not fragmented by channel. Clear executive accountability is needed to eliminate conflicting ownership and to drive consistency. Cross-channel training ensures operational teams understand evolving scam patterns and can apply playbooks wherever the customer interacts.

Shared scam playbooks create repeatable interventions and reduce variability. Enterprise management information is needed to measure effectiveness, so approaches can adapt quickly. Explainability is essential to justify decisions such as holds, declines or added friction, and to demonstrate reasonable steps. Cross-channel aftercare ensures the bank supports customers consistently and reduces repeat victimization risk.



A connected defense for an ever-evolving threat

> LexisNexis® Risk Solutions can help empower banks that choose to lead with an orchestrated, layered approach to scam prevention.

By combining vast networks of data with decades of subject matter expertise, behavioral and device intelligence, responsible AI-powered scam and mule detection models and real-time network insights, LexisNexis® Risk Solutions helps banks create a more connected strategy to detect risk earlier, intervene with greater confidence and protect customers from harm.

The future of scam prevention is not a single control, model or payment check. It is a **connected defense framework** that helps people live life more securely.

Find out more today.

Defense That Keeps Customers Safe

Scammers operate as intelligent, multi-channel networks. Banks have to do the same.





About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions provides customers with information-based analytics and decision tools that combine public and industry-specific content with advanced technology and algorithms to assist them in evaluating and predicting risk and enhancing operational efficiency. Headquartered in metro Atlanta, Georgia, the company has offices throughout the world, serves customers in more than 190 countries and territories and is part of RELX. For more information, please visit LexisNexis Risk Solutions.

Visit risk.lexisnexis.com for more.

This document is for informational purposes only and does not guarantee the functionality or features of any LexisNexis® Risk Solutions products identified. LexisNexis Risk Solutions does not represent nor warrant that this document is complete or error free.

LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc., registered in the U.S. or other countries. Digital Identity Network and ThreatMetrix are registered trademarks of ThreatMetrix, Inc., registered in the U.S. or other countries. Other products and services may be trademarks or registered trademarks of their respective companies.

Copyright © 2026 LexisNexis Risk Solutions.