Transaction Forensics

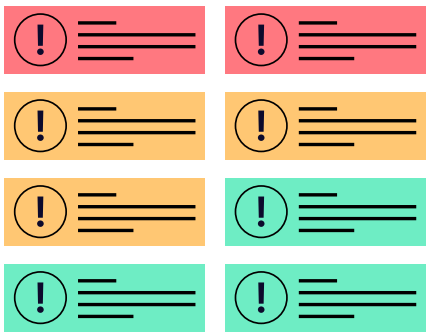
resistant ai
Case study

Transaction Forensics: The explainable AI add-on for your transaction monitoring system

Today's risk environments are evolving rapidly: new payment mechanisms, new financial products, and rapid geo-political shifts across markets are all opportunities for criminal behaviors. Rules-based systems are a necessity, but they aren't adaptable enough to keep up. Transaction Forensics from Resistant AI is the fast and cost-effective way to leverage the power of artificial intelligence without replacing the systems you already have in place.

How AI augments your rules-based system

Transaction Forensics sits between your existing transaction monitoring and case management systems, enriching both. The result: more productive analysts who spend their time investigating what counts and finding what's been slipping through.

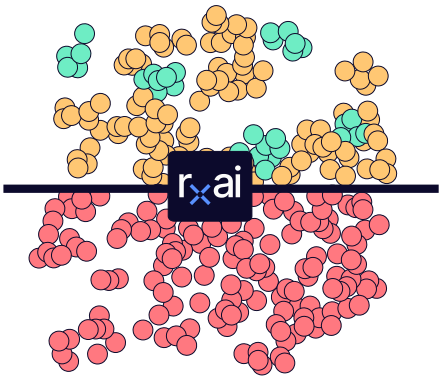


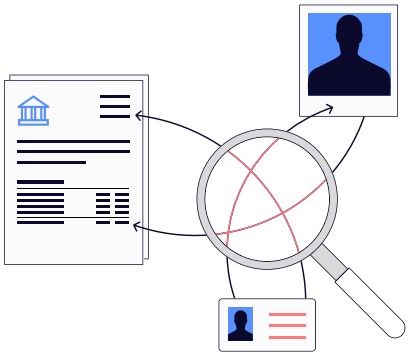
1 Alert Prioritization gets your alerts under control

Your system processes alerts as normal, then our AI kicks in. Alerts are sorted based on potential risk and served up to analysts with enriched details about each transaction: **categorize, prioritize, contextualize.** In seconds, Alert Prioritization pinpoints where analysts are most likely to find suspicious behaviors—with 99% of alerts resulting in SARs categorized as high- or medium-risk out of the box—and context gives them a head start understanding what's really going on. What's more, looking back at which alerts tend to land in which priority helps identify and optimize underperforming rules.

2 New Detections uncover what your rules are missing

We apply a diverse ensemble of anomaly detectors to the customer and transaction data you already collect. The outcome: a highly precise picture of the customer segments you serve and an excellent idea of what constitutes normal behavior for each. This means one-off anomalous activities or patterns of behavior that don't fit with existing groups stick out like sore thumbs to our detectors. This can triple the financial wrong doing you uncover in your system by highlighting everything from money mule networks to scams' starting points.





3 Go beyond reacting to financial crimes—prevent them

Making Resistant AI detections an integral part of your transaction stream attaches the benefits of AI to every action your customers take. In under 100 ms, you get high-precision predictive AI in real time: you can cut off layering attempts early and start investigations before the trail turns cold. You'll gain a reputation as the most well-protected financial service around—a boon for customers and a deterrence to criminals.

www.resistant.ai

Book a demo today

Transaction Forensics

resistant.ai
Case study

Changing the transaction monitoring game with an ensemble model approach

An ensemble approach employs not one grand model but layers of simpler models that highlight statistically anomalous behaviors across a range of dimensions. The result is modular groups of ensembles we call detectors that more precisely identify potentially criminal behaviors, whether we've seen them before or not.

Customization

Choose from over 60 detectors that identify and categorize risks, deploying them based on your unique needs. When a new trend is uncovered, new detectors can be assembled in as little as two weeks.

Explainability

Thanks to their narrow focus, each detection comes with a clear, readable description indicating why it appeared. This sets investigators off on the right track and makes reviews a breeze.

Easy maintenance

Never suffer from downtime. Modularity means you don't need to take the whole system offline to fine-tune the performance of specific detectors or launch new ones.

Behavioral typologies bridge gaps and expose complex activities

Transaction Forensics is loved by both fraud and AML teams: building information-rich identities breaks down departmental silos and strengthens overlapping responsibilities required to fight advanced risks. Here's an idea of the types of crimes you can catch by taking a united approach.

Authorized push payment (APP) fraud

Take out this fast-growing scam technique by cutting off the "money mules" it depends on.

Sanctions evasion

Go beyond PEP and sanctions lists to connect individual fronts based on behaviors.

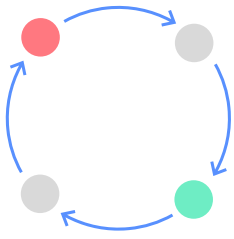
Human trafficking

Clearly see the funding patterns indicative of trafficking, such as repeating one-way travel arrangements.

How do we do this so effectively? Our detectors pinpoint sophisticated layering and structuring behaviors that elude simple rules. These are just some of the 60+ detectors that work together to detect financial crime:

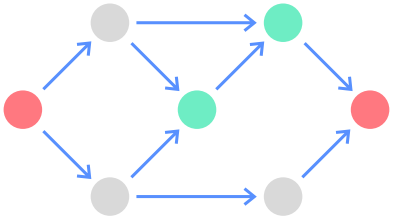
Cycling

Take out this fast-growing scam technique by cutting off the "money mules" it depends on.



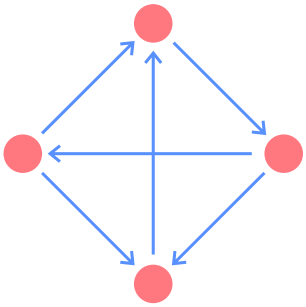
Split-merge

Detect layering when funds are split into various transactions sent from a single source, channeled through a number of intermediary accounts, and finally merged again in a single destination account.



Clique trading

Detect complex layering when similar amounts are traded back and forth throughout a network of related accounts.



What optimizing can do for you

Adapt to new markets
Focused fintech entered 5 new markets in just 6 months with better controls that revolutionized their risk-based approach.

Investigate real risks, efficiently
Prioritization and risk-based sampling of low-risk alerts helped a mid-sized EU bank reach 5x investigatory productivity.

Evolve with emerging threats
12 new behavioral typologies launched in 2 months.