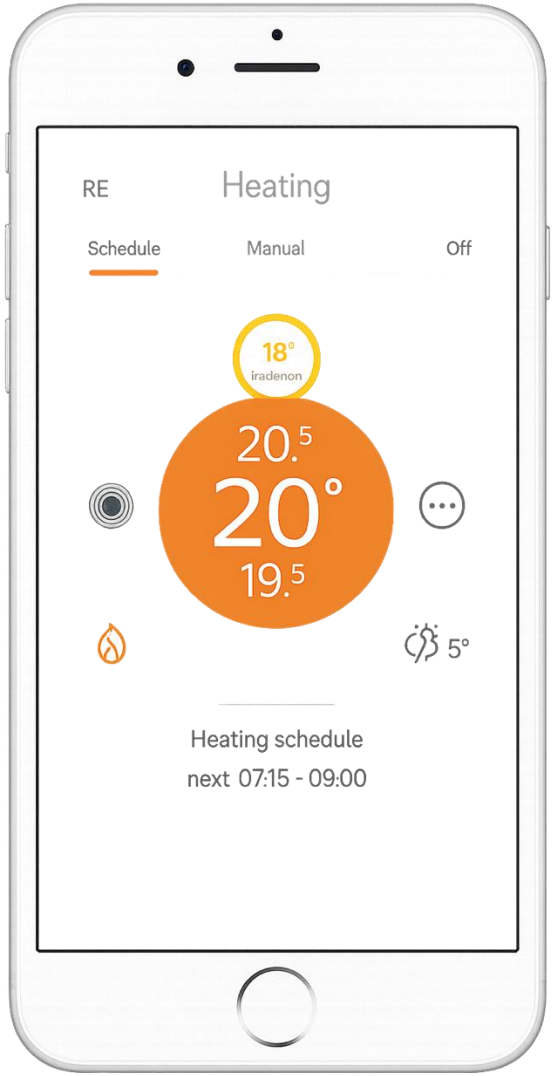
quantexa

From Alerts to Insight: Strategies for effective AML investigations and controls in the AI age

Juliet Robey
EMEA Financial Crime Solutions Manager

Confidential | Quantexa®



How we use technology in our personal lives

We change how we live to benefit from technology

“Customer behaviour and customer attributes… when combined with transactions, can provide a broader insight into potentially suspicious activity.”
Wolfsberg statement on "Effective Monitoring for Suspicious Activity (MSA) Part I: Moving Beyond Automated Transaction Monitoring”

“Understanding why the new approach (MSA) should be different by design, is crucial to avoiding low value-added comparisons between past and future performance. It should work in concert with the broader financial crime control environment. This may result in an approach that does not detect everything historically considered suspicious.”
Wolfsberg Effective MSA Part II: Transitioning to innovation

EBA and FATF have recently noted that whilst there are many benefits available through the adoption of “innovative technologies” within FinCrime programmes, unmanaged adoption can have adverse impacts. The new tech frequently outpaces the maturity of governance frameworks and the processes needed to manage associated risks and realise the operational benefits.

“75% of participating banks intend to invest in AI in future to improve TM.”
EY Nordic survey 2025

How we use technology in our professional lives

Limited re-orientation of goal setting or ways of working holistically

Agenda:

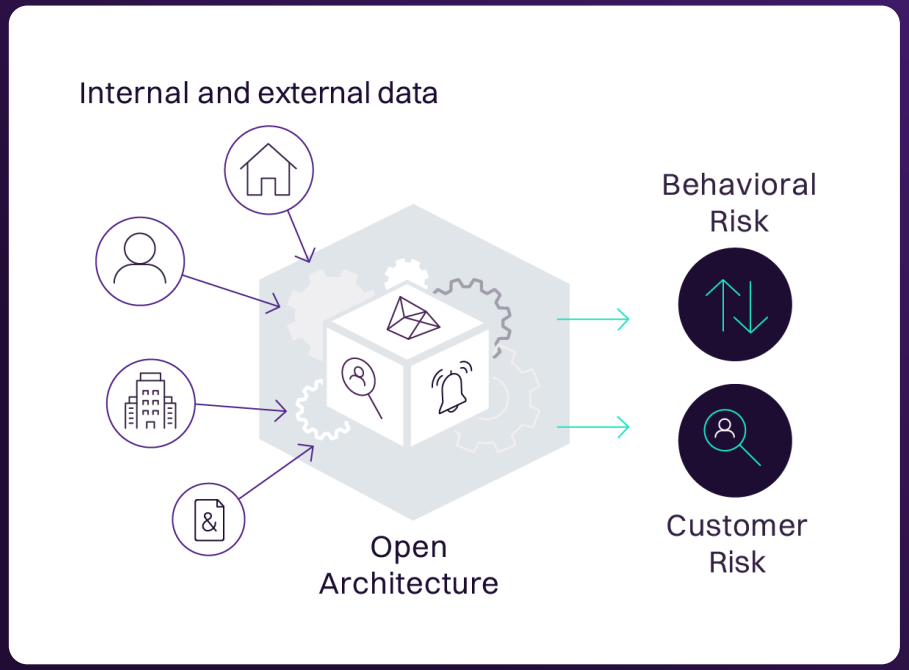
1. Defining Contextual Monitoring

2. AML Transformation journey for AI age
   - Detection
   - Investigation
   - Controls

3. Lessons Learnt and Key Takeaways

From Alerts to Insight: Strategies for effective AML investigations and controls in the AI age

What is Contextual Monitoring – FATF Definition



FATF

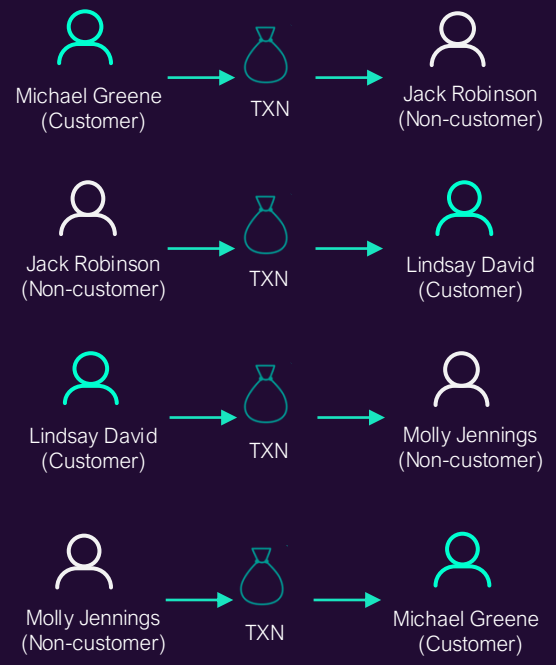
OPPORTUNITIES AND CHALLENGES OF NEW TECHNOLOGIES FOR AML/CFT

"Contextual Monitoring is the ability to join and connect together data from different systems and sources to create context and meaning to identify significant connections and improve accuracy. It employs advanced algorithms which allow more sophisticated scoring and analytical approaches."

The contextual difference

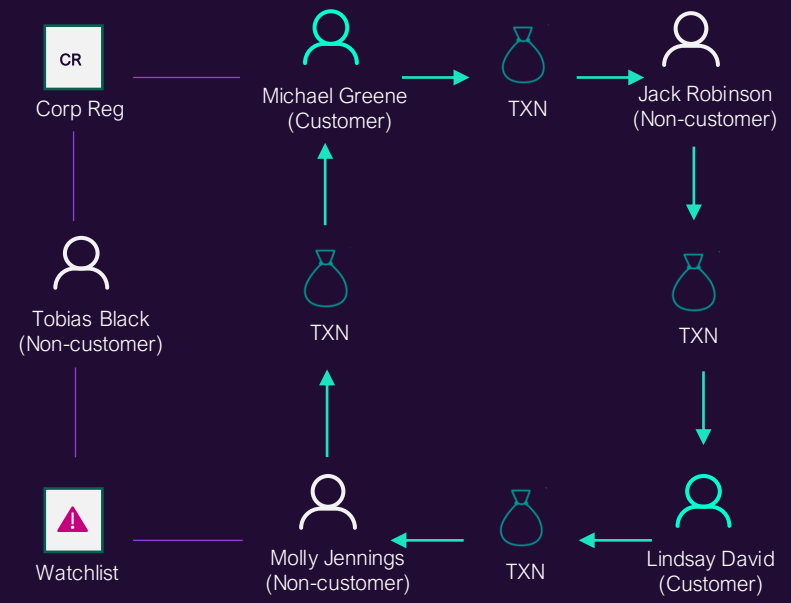
Traditional TM Systems

This is where the story ends for banks using traditional transaction monitoring solutions



Contextual Monitoring

Connecting all available data provides added context for customer and counterparty relationships to uncover crime



Quantexa empowers financial institutions to PROTECT their business from hidden risk OPTIMIZE detection with context-driven intelligence and confidently GROW by turning financial crime compliance into a strategic enabler for innovation and expansion

AML Transformation Journey for AI age

Detection

- Regulators encourage a more risk-based approach, integrating context into detection helps achieve this
- Whether using AI in Detection or not, contextual monitoring improves the quality of input to risk detection

Include **non-transactional** risk indicators into your detection.

Adopt a **many-to-one** input to alerting.

Integrate machine learning feedback into your detection **mindfully**

Investigation

- The investigation approach must evolve to support the technology transformation realising its full value
- All key parties should understand how the technology works to ensure cross-organisational support

Adopt a **structured, tiered standard** for reviewing non-transactional alerts on parties

Allow the **"who", "why", holistic context** to drive dispositioning alert not just transactional

Ensure **trust** is built in system decisions through testing and engagement involving **risk stewards, audit and regulators**

Controls

- Adapt control framework to ensure the detection goals are enabled and risks managed on an ongoing basis
- Quality testing, controls testing and independent model validation are still critical to a robust TM ecosystem

Ensure governance structure fit for **robust but agile decision making**

Create strong **feedback loop**

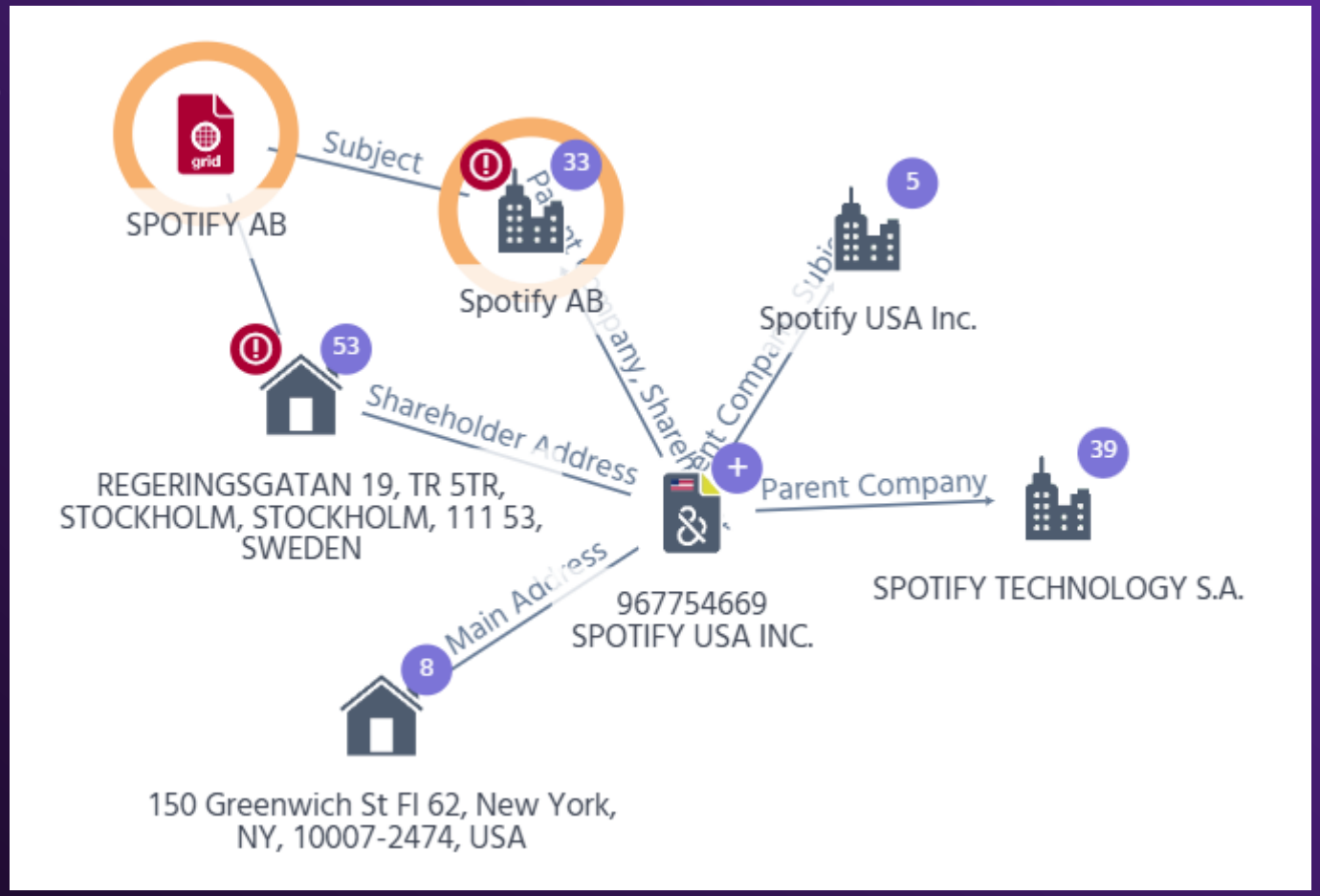
Review your **metrics for success** and ongoing quality monitoring

Investigating a lower risk alert with context quickly

There is evidence to suggest Swedish crime gangs use Spotify for their income, but not the same as Spotify itself laundering money. Important difference, is Spotify the alert subject or a counterparty, sending funds to the alert subject.

Alert on Spotify due to high value activity (imagined) and non-AML risk related watchlist hit linked to Russia. A review of the company and watchlist hit should lead to a very brief AAR before closing

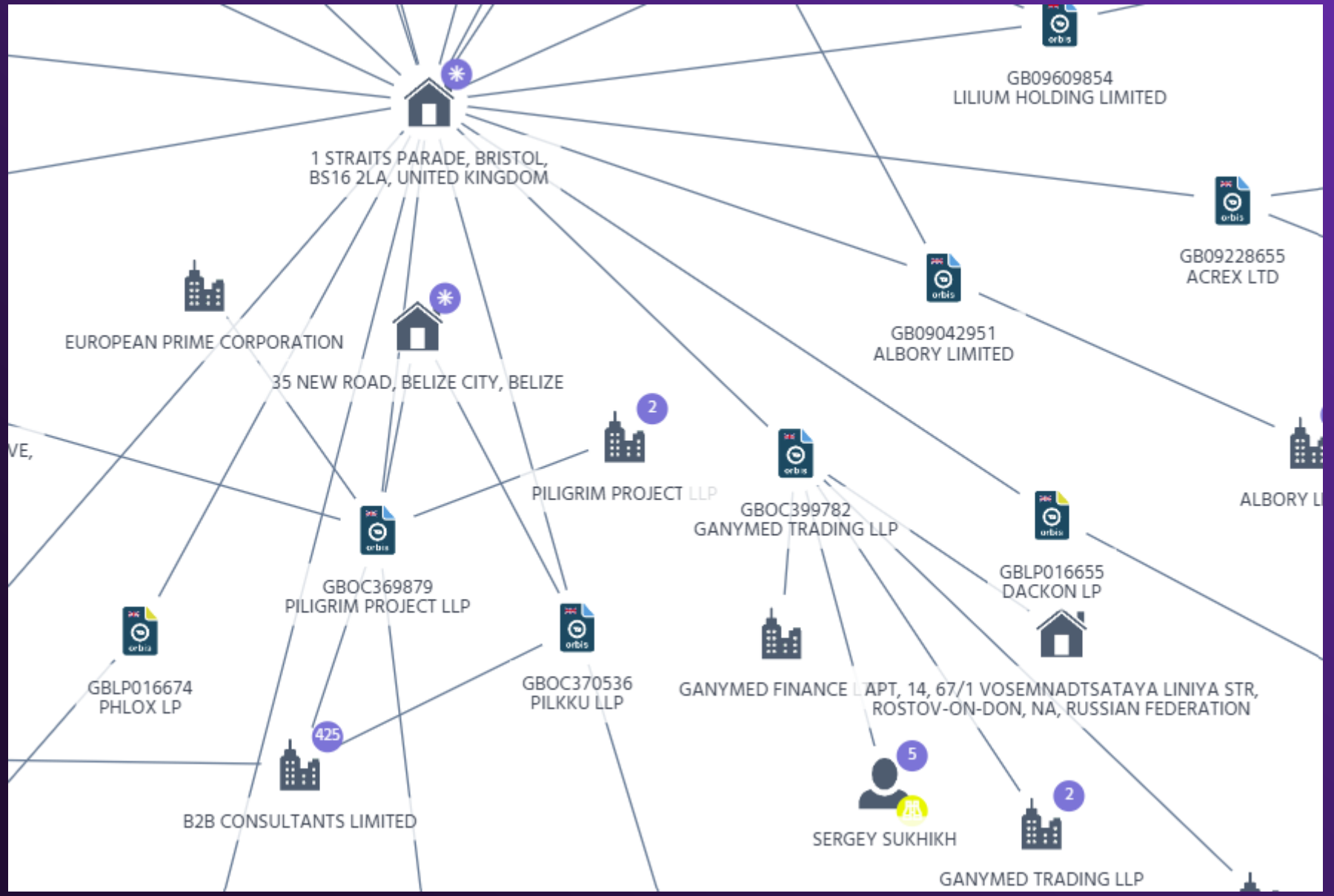
SOURCE	CATEGORY	SUBCATEGORY	DATE	DESCRIPTION
	Non Specific Crime	Fine - Less than $10,000	2022-07-28	A Moscow court has fined Spotify 500,000 rubles ($8,100) because of the company's failure to localize the data of Russian users on the country's soil.



Investigating a higher risk alert with context quickly

1 Straits Parade was exposed as being used as the registered address for companies, set up by middlemen on behalf of Eastern Europe clients who used them to establish shell companies to launder money

Alert due to an excess of LP/LLPs, high risk jurisdictions, all linked to a residential address are enough red flags to warrant an escalation without much account activity review



Lessons learnt

VALUE & MODELS	IMPLEMENTATION	DATA & INFRASTRUCTURE	INVESTIGATION
Agree on business value that can be achieved phase by phase and how to measure it	Involve all relevant user groups / stakeholders from the outset and throughout the project lifecycle	Assess data availability and quality as pre-requisite before full project kick off	Involve investigation SMEs in score design and UI design to ensure valuable two-way knowledge sharing
Maintain strict governance around how time/cost/scope/business changes impact agreed business value statements	Adopt an Agile implementation plan. Detailed solution design is best done post data work and in iteration with the users	Understand end to end data flow and put governance in place to be aware of upstream data/feed/system changes	Change procedures and overall mentality of what good looks like, "tickbox mentality" and what is the basis for SAR filing
Ensure business change vision is executed keeping pace with technology change	Ensure pre-implementation engagement and alignment with Model Risk Management/Governance processes	Invest in underlying data quality and ER and establish Cloud infrastructure dependencies early on	Consider the wider target operating model (teams, location strategy) and tooling (case management and MI)

Key takeaways

- Form a clear business change strategy before making any technology change decisions
- Invest in strong data foundations (data quality and ER) and infrastructure (Cloud)
- Assess how “AI ready” you are holistically (SAR outcomes, model risk management, risk appetite)

- Start with integrating context into your risk detection, it is suitable for every size of bank / use case
- Plan for Agile governance that engages required parties on targeted topics
- Engage independent model validation and regulators early in your transformation plans

- Anticipate the wider organisational engagement with the change, tell the transformation story
- Implement a robust 360˚ control framework that ensures risk exposure changes are assessed and technology fitness to meet the gaps is planned for and addressed
- Look for accountable and knowledgeable vendor partners to support your technology vision

Thank you.