Bitcast Brief 021 - Yenez Compliance (Subnet 54)

✨ Overview

Yanez Compliance (Subnet 54) tests and certifies financial crime prevention systems, providing compliance to banks and other financial institutions in a highly regulated environment.

The mission is to improve how financial institutions combat fraud and anti-money laundering when interacting with third parties.

💡 Why It Matters

- 🌍 $200B/year spent on financial crime prevention
- ⚠️ Compliance and testing is slow, manual, costly — MIID automates it in hours
- 🏦 Required by regulators → it is critical that third party fraud and anti-money laundering (AML) systems assist the banks in compliance

---

🏛️ Testing is a Foundational Pillar for Robust AML

Testing serves as a fundamental pillar of any Anti-Money Laundering (AML) program by providing independent assurance that the program's controls, policies, and procedures are functioning effectively to detect and prevent money laundering activities.

Testing to spot gaps in:

- Transaction monitoring calibration
- Customer due diligence
- Suspicious activity reporting
- Staff training

Typically conducted by **internal audit, compliance teams, or third parties to help banks and other regulated financial entities**:

- **Meet regulatory requirements**
- **Avoid penalties, reputational damage, and illicit activity exposure**.

*See the “Regulators’ Stance on Testing & Auditing” section in the further reading section for more information.

💰 How much is spent on compliance

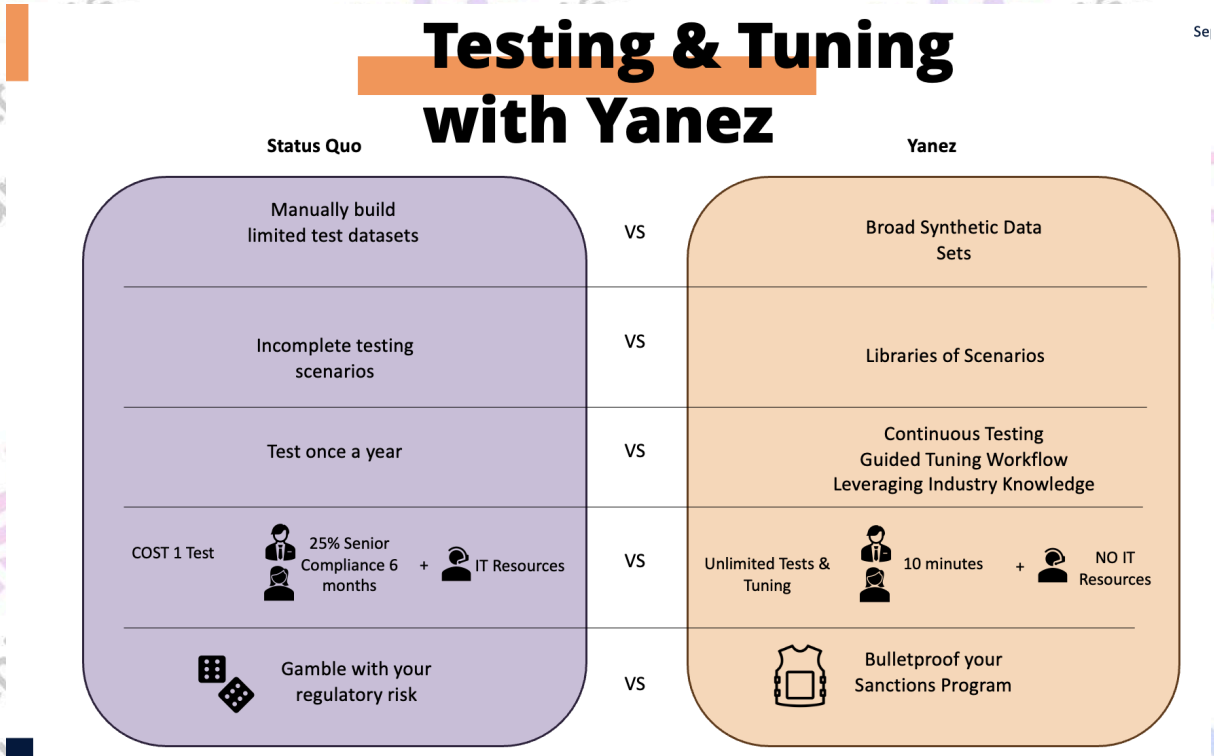
- A study by LexisNexis Risk Solutions, shows that financial crime **compliance costs** are around **$61 billion per year** in the United States and Canada source
- Globally, the **total cost of financial crime compliance** was reported at approximately **$274 billion in 2022**, up from $213.9 billion in 2020 source

💵 Fines:

- $321B in fines source

🛠️ vs 🤖 Manual testing vs Yanez’s AI-powered subnet automation

& How Yanez is uniquely positioned to disrupt the market



- **Data Quality:**
    - Yanez test data is comprehensive, and configurable to the risk profile of the organization. Both the tests and the insights from the results are meaningful to the organization.
    - Current technology to test systems are generic and disregard the nuances of the organization causing several irrelevant results. For manual processes it is too costly to produce and implement broad coverage of cases.

- **Metric Framework:**
    - Yanez provides a quantitative framework to accurately score the performance of financial crime prevention systems. These metrics can be used as a benchmark which gives a clear framework for measuring improvement.
    - Current testing systems don't provide a framework where improvement is easily achieved.
- **Decentralized Intelligence:**
    - The Bittensor protocol's distributed workforce can leverage resources across the world wherever the intelligence exists. It enables every skilled resource no matter where they are to be part of the intelligence network.
    - No competitor in the market has this capability.
- **Infinite Scale:**
    - Scales without exponential expense to the organization, ensuring diverse, high-quality data to meet regulatory demands
    - Centralized systems cannot achieve this.
- **No IT Dependency:**
    - Compliance teams, and financial crime prevention teams have restricted access to internal IT resources. Yanez offers all the functionality without requiring IT resources from the organizations. This is very hard to replicate as it is a fundamental aspect of the go to market strategy and the design of the platform. Yanez has achieved partnerships with sanctions screening providers covering over 75% of the market.
    - No other competitor in the market has this approach.

- **Full Workflow Approach:**
    - Yanez focuses both on finding the potential gaps in the system and in how to help the teams address such problems.
    - No other competitor provides the proper support for operational workflows to resolve the issues that it finds.

*See the “In depth: current manual processes that Yanez is replacing” section in the further reading section for more information.

📊 Market Opportunity

- $12B addressable market in next 5 years
- Expansion from sanctions into → KYC, adverse media, transaction monitoring

---

⚔️ Competitive Edge

- Client-first vs regulator-first approach
- Patents protect logic layer
- Plug-and-play with existing sanction screening providers

📈 Growth & Traction

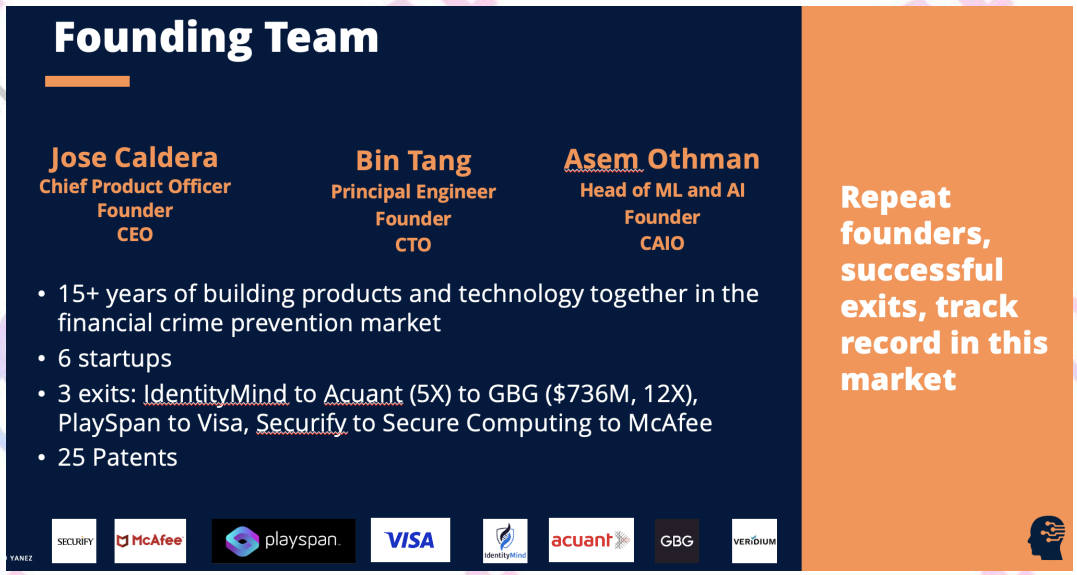
- Product launched Oct 2024
- Multi-billion-dollar financial organizations onboarded
- $900K raise (oversubscribed)

🚀 Roadmap & Vision

- 2025–2026: Expand to KYC, transaction monitoring for fraud and money laundering, adverse media
- Focus on growth + sticky clients, not burns

👥 Founder & team

- José Caldera (ex-IdentityMind, 20+ years in compliance)
- Lean, experienced team in AML + financial crime prevention



🤝 Partnerships & Integrations

- Major sanction screening provider partnerships
- Exploring subnet collaborations (Bitmind for AI video security tools etc.)

🔗 Resources

- Website: www.yanezcompliance.com
- X (Twitter): @yanez__ai
- Revenue Search Interview - YouTube
- Docs / Whitepaper: https://www.yanezcompliance.com/post/managing-banking-as-a-service-baas-third-party-risk-part3

📬 Contact

- DM via X: messages

📖 Further reading

Regulators' Stance on Testing & Auditing

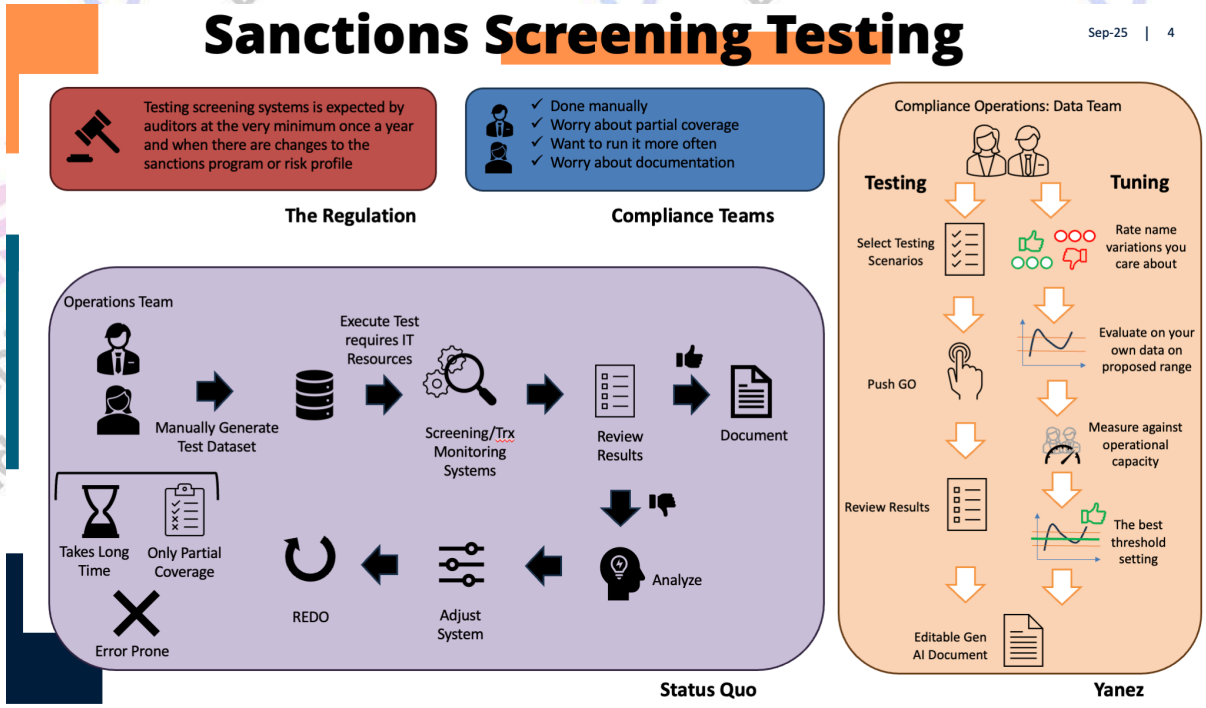
OFAC

- **Regular Testing**: End-to-end testing of sanctions screening systems, data inputs, and compliance processes.
- **Independent Audits**: Sufficiently resourced, accountable to senior management, used to identify and remediate weaknesses.
- **Remediation**: Enforcement actions often cite weak testing/auditing; settlements typically require stronger independent testing, audits of high-risk relationships, and ongoing monitoring.

FinCEN

- **Pre-Implementation**: Risk reviews, data conversion, integration testing, and readiness checks before systems go live.
- **Post-Implementation**: Ensure systems meet design objectives, operate effectively, and protect against ML/TF risks.
- **Model Validation**: Confirm thresholds, limits, parameters; review governance, source data, and alert output.
- **Documentation & Governance**: Clear documentation of design, vendor assumptions, filtering logic, and update processes.
- **Periodic Updates**: Regular assessment of matching technology, sanctions lists, and thresholds.
- **Audit Programs**: Review risks, controls, conversion/testing, and post-go-live results.

Current Process flow (status quo) of sanctions screening vs Yanez



Key activities in manual testing and tuning:

- **Review alerts**: Analyze true positives, false positives, and false negatives across entity types, transactions, and regions.
- **Evaluate algorithms**: Check fuzzy matching calibration (names, phonetics, nicknames, addresses) to balance detection and minimize false alerts.
- **Adjust parameters**: Work with IT to refine similarity scores, geographic settings, and exception lists.
- **Iterative testing**: Re-run historical data to measure improvements in detection and false positive reduction.
- **Scenario testing**: Use synthetic transactions with name variations, alternative spellings, and address formats to test evasion detection.
- **Sanctions list updates**: Validate system performance immediately after list changes to ensure new designations are integrated.

In depth: current manual processes that Yanez is replacing

The manual testing and tuning process begins with sanctions analysts conducting systematic reviews of the screening system's performance by analyzing both true positives (legitimate matches) and false positives (incorrect matches) generated by the automated

screening filters. Analysts typically start by examining a representative sample of alerts across different entity types, transaction patterns, and geographic regions to understand how the system is performing against various sanctions lists including SDN, sectoral sanctions, and consolidated screening lists. They evaluate whether the fuzzy matching algorithms are appropriately calibrated by reviewing cases where sanctioned parties were missed (false negatives) or where legitimate customers generated excessive alerts due to overly sensitive matching parameters. This involves manually comparing customer names, addresses, and other identifying information against sanctions list entries to determine optimal threshold settings for name matching, phonetic algorithms, and nickname variations.

During the tuning phase, analysts work closely with IT teams to adjust screening parameters based on their findings, such as modifying similarity scores for name matching (typically ranging from 70-95% depending on risk tolerance), refining geographical proximity settings, and updating exception lists for common false positive generators like generic company names or popular personal names in specific regions. They conduct iterative testing by running historical transaction data through the newly calibrated system to measure improvements in detection rates while monitoring false positive reduction. Analysts also perform scenario-based testing by creating synthetic transactions involving known sanctioned entities with slight name variations, alternative spellings, or different address formats to ensure the system can detect evasion attempts. Additionally, they regularly test the system's ability to screen against updated sanctions lists by processing control transactions immediately after list updates to verify that new designations are properly integrated and existing entries remain active. This ongoing manual process ensures that the screening system maintains optimal performance while balancing compliance effectiveness with operational efficiency.