Celent.
a GlobalData company

Zenus Bank:

Embedded Compliance at Global Scale

Winner of the 2026 Celent Model Risk Manager Award for Operational Resilience

Ian Watson

June 11, 2026

Contents

Case Study at a Glance

Zenus Bank built a fully embedded, real-time compliance and fraud management infrastructure to power its global embedded banking platform. Starting as a direct-to-consumer bank in Puerto Rico, Zenus pivoted to become the first U.S. business-to-business-to-consumer (B2B2c) bank to offer embedded accounts in over 180 countries, providing fintechs, EMIs, MSBs, broker-dealers, and foreign banks with USD accounts, cross-border payments, and Visa card issuance. The compliance and fraud stack is not a layer sitting alongside the platform; it is part of the platform. With embeded compliance as an accelerator, Zenus exceeded $4B in monthly total payment volume (TPV), and grew its partner network to more than 1,300 institutions within its first year of full launch.

Table 1: Case Study at A Glance	
Financial Institution	Zenus Bank
Initiative	Zenus Embedded Compliance
Synopsis	Zenus built a fully embedded, real-time risk, compliance, and fraud management infrastructure to enable the growth of its B2B2C banking business. Combining 3rd party applications with a proprietary risk engine, the bank enforces AML, KYC/KYB, and anti-fraud controls during onboarding and at the point of transaction
Timelines	The project took a little over a year, as Zenus pivoted from a direct-to-consumer bank to a B2B2C embedded banking infrastructure provider, with a soft launch in February 2024 and full launch in March 2025.
Key Benefits	• 6,000+ monthly compliance investigations • SAR filings from 100 annually to 200+ per month • $2 million in client fraud losses recovered • Partner onboarding went from months to under one week
Key Vendors	NICE Actimize (AML, fraud and case management); Exiger (TPRM); Tuum (core banking); Onfido (identity verification); Chainalysis (blockchain analytics); J.P. Morgan (settlement); Visa (card network); Microsoft Azure; Purpleplum (white-label digital banking and onboarding platform)

Source: Zenus Bank

Celent Perspective

Zenus Bank's initiative stands out because it treats compliance not as a control layer around the business, but as the infrastructure that makes the business possible. The bank's embedded banking model depends on its ability to provide U.S.-based accounts to international financial institutions across more than 180 countries. That model cannot scale through conventional onboarding queues, post-transaction monitoring, and manually coordinated risk reviews. Zenus redesigned the compliance architecture around the operating model rather than forcing the operating model through a traditional compliance process.

The most distinctive element is the orchestration layer and the way it connects onboarding, transaction monitoring, third-party due diligence, identity verification, sanctions screening, and fraud controls. Zenus's proprietary risk engine sits at the center of that architecture, normalising data across systems, applying consistent risk logic, and enforcing decisions in real time. The bank did not simply assemble a set of strong vendor tools. It created a control fabric that allows those tools to operate as one platform.

The results show why that architecture is commercially important. The speed and versatility of embedded compliance, underpinned Zenus' rapid growth to more than $4B in monthly payment volume, a $75B annualised payment volume run rate, while real-time monitoring helped recover $2–3M in client fraud losses. These metrics show a compliance function that is scaling with the business rather than operating as a brake on it.

The broader lesson is that operational resilience is not only about avoiding disruption. In this case, it is what makes the business model work. Zenus has demonstrated that a smaller bank can compete in complex cross-border markets by making risk infrastructure a source of differentiation. The project earns recognition because it links regulatory control, operational scalability, and commercial growth in a single risk and compliance architecture.

Detailed Description

Introduction

Zenus Bank is a US-chartered bank headquartered in Puerto Rico. Founded in 2019 as a direct-to-consumer digital bank, it pivoted to become an infrastructure bank: a B2B2C platform providing USD accounts, cross-border payments, and Visa card issuance to fintechs, money-service businesses (MSBs), and foreign banks in 180+ countries. In collaboration with the UNEP FI (United Nations Environment Programme Finance Initiative) initiative, Zenus enables clients to responsibly access high-risk and underbanked markets while maintaining strong compliance and financial integrity standards. The initiative profiled here is the compliance and fraud infrastructure that makes that platform operable at scale

Table 2: Company Snapshot	
Year Founded	2019
Headquarters	San Juan, Puerto Rico
Total Assets	Under $1 billion (Tier 6)
Geographic Presence	Embedded accounts available in 180+ countries;
Employees	70+
Other Key Metrics	1300 direct Financial Institutions
Relevant Technologies and Vendors	NICE Actimize, Tuum, Exiger, Chainalysis. Purpleplum
Source: Zenus Bank	

Opportunity

Zenus identified a clear gap in global financial infrastructure: many international fintechs, EMIs, MSBs, broker-dealers, and foreign banks need access to U.S. accounts, payments, and card issuance, but lack a practical path to obtain them. Traditional correspondent banking is slow, expensive, and increasingly constrained by de-risking. For many institutions in emerging markets or higher-risk corridors, compliant access to USD banking has become a structural bottleneck.

The opportunity was to turn that bottleneck into a platform business. Zenus set out to provide embedded U.S. banking through APIs, allowing qualified institutions to offer USD accounts, cross-border payments, and Visa cards without building their own U.S. banking infrastructure. That required more than a digital front end. It required a compliance and fraud architecture strong enough to support institutional onboarding, real-time transaction monitoring, and multi-jurisdictional risk controls at scale.

Three operating problems shaped the initiative:

1. Onboarding international financial institutions through manual diligence cycles could take months, which was too slow for an embedded banking model.
2. Conventional fraud and AML tools available to a smaller bank were not built for Zenus's transaction volumes, payment-rail diversity, or geographic reach.
3. Legacy correspondent banking data flows, especially SWIFT messages, often lack the counterparty detail needed for modern monitoring.

The initiative's executive sponsor is Gabriel Viera, Chief of Compliance at Zenus Bank. Viera has led the programme from its initial framing through to the current operating platform, and is direct about what the bank set out to build. "The reason we created Zenus Bank was to make cross-border payments and opening accounts safer and secure for our customers, and to hit the right balance between the user's journey and being compliant with the rule of law," he explained. "What we designed is a way of creating an infrastructure bank where we can provide other financial institutions the infrastructure to be compliant."

Zenus's ability to provide embedded U.S. banking service was reliant on building the risk management infrastructure that could make that access commercially and regulatorily viable.

Solution

Zenus built the compliance and fraud stack directly into its embedded banking platform. The architecture centers on a proprietary orchestration layer and risk engine that connects core banking, third-party due diligence, transaction monitoring, identity verification, blockchain analytics, settlement, and card issuance into a single control environment. The objective was not to bolt compliance onto the platform, but to make risk evaluation part of every onboarding decision, account event, and transaction.

Three systems form the core of the platform. Tuum provides the cloud-native core banking engine. EXIGER TPRM automates institutional due diligence. NICE Actimize Essentials provides continuous transaction surveillance across ACH, FedWire, SWIFT, card, and stablecoin activity, with machine-learning AML models, behavioral anomaly detection, sanctions screening, and case management.

Zenus's proprietary orchestrator and risk engine normalizes data across these systems, calculates dynamic risk scores, applies BSA/AML and USA PATRIOT Act rules, and enforces decisions in real time. Says Viera, "The orchestrator we built inside is the heart of the bank. It communicates with all systems. The uniqueness of this bank is the integration layer we built".

Partner information flows through the orchestrator, which routes data to the appropriate system for onboarding or payment processing. Risk thresholds, fraud rules, AML parameters, and partner profiles can be updated in minutes. For example, Actimize's customer due-diligence (CDD) module receives real-time KYC applications from the Zenus risk rating engine and returns customer risk ratings synchronously.

Implementation

The initiative was delivered by a 38-person core team:

- 28-person Compliance and Financial Crime team (AML analysts, KYC/KYB specialists, sanctions officers, fraud analysts, and regulatory experts)
- 10-person Technology team (engineers, DevOps, information security specialists, and product managers).

The team operated under a unified governance model, with Compliance, Engineering, and Product aligned on a shared continuous-delivery cadence. The absence of a compliance-versus-engineering boundary is how the platform achieves the "minutes-to-deploy" cadence on rule changes.

Not every part of the build went to plan. The early construction of the payments stack surfaced a problem that would go on to shape the bank's vendor policy. Zenus had contracted an external provider to build a SWIFT platform on the logic that an early-stage vendor would be cheaper and faster than an enterprise-grade alternative. In practice, the vendor had neither the operational capacity nor the domain expertise to build one.

Gabriel gave the following example, "We hired an entity to build us a SWIFT platform, and in the second meeting after we signed the contract, the had a question. 'What is

SWIFT?' I'm not kidding." Navigating around this consumed internal resources that had been scoped for other parts of the platform, delayed the payments roadmap, and eventually cost more than a mature provider would have charged in the first place.

Table 4: Technology Partners Responsibilities and Resources

Company	Support
NICE Actimize	Continuous transaction surveillance across ACH, FedWire, SWIFT, card, and stablecoin rails. Delivers machine-learning AML models, behavioural anomaly detection, sanctions screening, and Generative AI-assisted case narration.
Tuum	Cloud-native core banking engine. Provides the ledger and virtual account architecture, multi-entity product orchestration, and high-volume transaction processing.
EXIGER TPRM	Third-party risk management and due diligence. Automates KYB/KYC checks, UBO mapping, and sanctions intelligence across 240+ jurisdictions. Provides Wolfsberg-aligned questionnaires.
Onfido	AI-driven biometric identity verification. Provides document fraud detection and liveness scoring for KYC onboarding.
Chainalysis	Blockchain analytics for crypto-adjacent transaction monitoring, wallet attribution, and illicit activity detection on USDC / Ethereum rails.
J.P. Morgan	Institutional settlement, liquidity management, and USD clearing for real-time cross-border payment flows.
Visa	Global card issuance, cross-border transaction processing, and BIN Sponsorship via Visa Principal Membership.
Purpleplum	White-label digital experience platform with omni-channel UI/UX delivery.
Microsoft Azure	Cloud and AI backbone. Provides hyperscale infrastructure, SIEM/SOAR via Azure Sentinel, and Confidential Compute.

Source: Zenus Bank

The effect of this experience was a redrawing of the build-versus-buy line. Components that define the platform's differentiation, most visibly the orchestration layer and the proprietary risk engine, were built in-house. Third-party dependencies are confined to enterprise-grade providers whose operating scale, audit posture, and regulatory experience match the profile of a bank processing cross-border flows at this volume. The current stack, Tuum, NICE Actimize, EXIGER, Onfido, Chainalysis, J.P. Morgan, Visa, Purpleplum, and Microsoft Azure, reflects that discipline.

Results

The results matter because they combine commercial scale with compliance throughput. Within the first year of full operation, Zenus reached a $75B annualized payment volume run rate, sustained more than $4B in monthly TPV, and supported 70% month-over-month transaction growth during 2025. The compliance infrastructure scaled with the business rather than slowing it down.

Detection and operational efficiency improved at the same time. SAR filings increased from 100 per year to more than 200 per month, reflecting greater monitoring capacity at scale. Zenus also recovered $2–3M in client fraud losses and compressed partner onboarding from months to under one week, turning compliance execution into a direct source of commercial advantage.

Table 5: Success Metrics

Benefit	**Results**
Cost reduction	Partner onboarding compressed from up to six months to under one week. eliminating the manual compliance review cycle Real-time monitoring recovered $2–3M in client fraud losses. A 28-person compliance team now manages 6,000+ monthly investigations.
Business efficiency	Real-time KYC, sanctions, fraud, and transaction decisioning replaced post-transaction batch review. SAR filings increased from 100 annually to 200+ per month, reflecting higher detection throughput. Individual clients scaled from $10M/month to $100M/month in processing volume.
Return on investment	With embedded compliance in place, Zenus reached a payment volume run-rate $75B per year, grew accounts 300%, and expanded to 1300+ financial institutions, fintechs, and corporate partners.
Strategic positioning	Zenus became the first U.S. bank to offer embedded accounts in 180+ countries, including higher-risk markets underserved by traditional correspondent banks.

Source: Zenus Bank

To evaluate monitoring efficiency and investigative precision, Zenus benchmarked its alert conversion performance against broader industry ranges. In 2025, the bank achieved a 16.2% alert-to-case conversion rate, within the typical industry range of 10–30%, while significantly outperforming benchmark ranges in higher-value investigative outcomes, with a 46.3% case-to-SAR conversion rate compared to an industry norm of 10–30%, and a 7.5% alert-to-SAR conversion rate versus the typical 2–5% range. These results indicate a comparatively high level of precision in alert

triage, case selection, and suspicious activity identification across the bank's compliance operations.

In May 2026, Zenus's compliance and fraud monitoring infrastructure successfully identified and stopped an attempted $700 million business compromise fraud scheme. The incident, which originated through a phishing-based social engineering attack, demonstrated the platform's ability to detect and intervene in complex cross-border fraud activity in real time before funds were transferred. As a result of the rapid intervention and coordinated compliance response, the funds were successfully returned to the victim within three days.

Lessons Learned

Zenus identified four lessons from the initiative:

Strategic clarity matters early. The pivot from D2C banking to B2B2C embedded banking changed the platform's requirements. Locking the strategy earlier would have reduced architectural rework and improved speed. Individual lessons learned:

- finalize a unified strategic blueprint at the outset
- document decision principles to guide trade-offs
- codify non-negotiables in a living Vision Charter

Speed and bank-grade control can coexist. To balance rapid innovation with regulatory rigor, Zenus found that the fastest path to operating at scale was to embed compliance, fraud, and security controls from the start rather than retrofit them later. Individual lessons learned:

- adopt agile delivery for speed
- embed compliance and security controls from day one
- harden infrastructure in parallel with feature development

Define operating workflows early. Onboarding, reconciliation, architecture governance, and risk decisioning should be mapped before scale-up. Individual lessons learned:

- Map onboarding, reconciliation, and support processes upfront
- Adopt standardized architecture councils and readiness gates from day one
- maintain a unified risk and decision log

Develop differentiating capabilities in-house. Zenus learned to build differentiating components in-house, like the orchestrator and risk engine, while relying on mature third parties for core capabilities. Individual lessons learned:

- Consolidate core functions under one roof for speed and coherence
- Build differentiating technology in-house whenever feasible
- Vet outsourced vendors carefully to make sure they don't overpromise on timelines and minimize integration realities

Path Forward

With a strong focus on AI-driven automation, adaptive compliance and global scale, Zenus has the following items on its roadmap.

AI-driven fraud and AML intelligence. Machine learning models will be deepened to enhance fraud detection accuracy, reduce false positives, and automate complex AML and due diligence workflows across all payment rails.

Adaptive, risk-based compliance models. The platform will expand dynamic compliance frameworks that adjust automatically to partner risk profiles, transaction behavior, and evolving global regulatory requirements, moving from rule-based controls toward context-sensitive risk assessment.

End-to-end workflow automation. Continued investment in automation will further compress onboarding, monitoring, investigation, and case management cycles, allowing Zenus to scale transaction volumes and partner growth without proportional increases in compliance headcount.

Generative AI for AML investigations. Zenus will deploy NICE Actimize's InvestigateAI capability alongside its internal Copilot and ChatGPT usage to synthesize alerts, transaction histories, and customer risk data into structured, analyst-ready case narratives. Deployment begins with a post-transaction MVP and is expected to move into real-time monitoring once sanctions-screening accuracy is proven; the bank has been explicit that AI errors in sanctions contexts carry unacceptable risk.

Global infrastructure and API orchestration expansion. Additional payment connectivity, expanded jurisdiction coverage, and strengthened API orchestration will support higher partner volumes and more complex cross-border use cases, including deeper integration with Visa, J.P. Morgan, and additional settlement partners.

White-label banking solution. Through Purpleplum, Zenus will deliver a fully integrated white-label platform combining USD account capabilities (ACH, wire, and stablecoin payments), card program management, and compliance-as-a-service, enabling partners to launch and scale end-to-end banking experiences under their own brand.

Conclusion

To serve an international, institutional, and compliance-sensitive client base, risk controls cannot sit outside the platform. By embedding compliance directly into onboarding and transaction execution, Zenus has made it part of the core infrastructure. That design choice allowed the bank to compress partner onboarding, support rapid growth, and maintain a single risk control environment across a highly complex international footprint.

The broader lesson is that operational resilience is not only about avoiding disruption. In this case, it is what makes the business model work. Zenus's platform demonstrates how a bank can use real-time risk orchestration, disciplined vendor integration, and an embedded risk operating model to serve markets that traditional correspondent banking often avoids. The result is a compliance architecture that protects the institution while enabling growth, which is precisely why this initiative stands out.

Leveraging Celent's Expertise

If you found this report valuable, you might consider engaging with Celent for custom analysis and research. Our collective experience and the knowledge we gained while working on this report can help you streamline the creation, refinement, or execution of your strategies.

Support for Financial Institutions

Typical projects we support include:

Vendor short listing and selection. We perform discovery specific to you and your business to better understand your unique needs. We then create and administer a custom RFI to selected vendors to assist you in making rapid and accurate vendor choices.

Business practice evaluations. We spend time evaluating your business processes and requirements. Based on our knowledge of the market, we identify potential process or technology constraints and provide clear insights that will help you implement industry best practices.

IT and business strategy creation. We collect perspectives from your executive team, your front line business and IT staff, and your customers. We then analyze your current position, institutional capabilities, and technology against your goals. If necessary, we help you reformulate your technology and business plans to address short-term and long-term needs.

Support for Vendors

We provide services that help you refine your product and service offerings. Examples include:

Product and service strategy evaluation. We help you assess your market position in terms of functionality, technology, and services. Our strategy workshops will help you target the right customers and map your offerings to their needs.

Market messaging and collateral review. Based on our extensive experience with your potential clients, we assess your marketing and sales materials—including your website and any collateral.

Related Celent Research

Dimensions: Risk & Compliance IT Pressures & Priorities
April 2026

Resilience Moves from Program to Performance
April 2026

Agentic AI Supercharges Regulatory Change Management
November 2024

Know Your Customer Systems: Customer Due Diligence / Customer Life Cycle Management — Technology Capabilities Matrix and 2026 XCelent Awards
February 2026

Know Your Customer Systems: Identity Verification — Technology Capabilities Matrix and 2026 XCelent Awards
January 2026

Risk & Compliance: Technology Trends Previsory; 2026 Edition
November 2025

Crypto Investigative Tools for AML & Anti-Fraud: Blockchain Compliance Solutionscape and Technology Capabilities Matrix
November 2025

Building Trust with Technology: Anti-Fraud Solutionscape and Technology Capabilities Matrix
September 2025

Copyright Notice