EPISODE 3 | Case File

Turning Risk Management Into Revenue

JANUARY 26, 2026

This transcript was auto-generated and may contain errors or inaccuracies.

Jeff Welcome to “What the F Happened? Fraud and Financial Crime Deconstructed”, a DEFEND podcast where we break down what's actually happening across fraud, scams, AML, and financial crime.

Emily Each episode cuts through the noise to explain the tactics, trends and real world impact behind the headlines so you're better prepared for what comes next. Let's get into it.

Jeff So, you know, if you've ever had to manage a budget, you know, this pain point we're diving into today, the whole risk management department security fraud compliance. It's usually just seen as this, uh, massive necessary cost center. You're spending millions just to stop bad things from happening, right?

Emily It's purely defensive.

Jeff Exactly. But our sources today, they tell this fascinating story about a leading payments processor that just completely flipped that script.

Emily Oh, completely.

Jeff They took their internal risk infrastructure specifically for fraud and AML. FRAML, they call it FRAML framework, and they transformed it from this, you know, operational drain into a strategic incremental revenue generator.

Emily Which is I mean, that's the holy grail, right?

Jeff It really is. So we're going to be unpacking the technical foundations that made this possible. We're talking unified systems, ensemble machine learning. And uh, this really critical architecture decision called multi-tenancy.

Emily That's the key.

Jeff It is our mission for you, the listener, is to walk away understanding not just how to tighten security, but how that security can be engineered to become a high value product you can actually sell.

Emily And you have to establish the scale here right away, because the complexity of the challenge. I mean, it's what dictated this whole radical transformation.

Jeff We're talking huge volumes, huge.

Emily We're talking about a leading merchant acquirer, a payment processor handling just an immense volume. Our sources say over sixty million transactions every single month.

Jeff Wow.

Emily Yeah. And that's for an ecosystem of more than two thousand five hundred clients. Think major retailers, downstream fintechs, financial institutions.

Jeff So in that world, the margins are tiny, razor thin.

Emily You're operating in this low margin environment where protecting your existing revenue from fraud while simultaneously controlling your operating costs. That's the central tension of the business.

Jeff You can't afford delays.

Emily You simply can't. The pressure to get the risk decision right in milliseconds, every single time. It's just immense.

Jeff That environment, it just sets the stage perfectly. But what was the tipping point? What forced them away from, you know, the comfort of their established home grown system?

Emily Well, the starting problem was classic. They were relying on these legacy in-house fraud systems.

Jeff Everyone builds it first.

Emily Exactly. And as their customer base and their transaction volume just exploded the old system, it just couldn't evolve fast enough to keep pace with modern, sophisticated attacks. It was an operational bottleneck. And it was threatening their growth.

Jeff So when a new fraud pattern emerged.

Emily Their response was delayed. And their customers, the merchants, they were the ones feeling the heat. It led to complaints to operational pressure for faster solutions. This wasn't just about losing money.

Jeff Now it's about losing trust.

Emily Exactly. Losing customer trust and hindering future acquisitions.

Jeff And the company's leadership. They summarize this so perfectly in the source material. They said, and I'm quoting here, we needed a single platform that could handle fraud and AML decisions in real time at massive scale, real time.

Emily That's the key phrase.

Jeff It is. And they add, we started to see the decrease in fraud exposure from month one. So that quote, it just perfectly frames the goal. Unified control, high speed, immediate impact. Right. But what I find most insightful is that they didn't just see a problem to fix, they saw an asset to sell.

Emily Yes, that's the strategic leap. They recognize the defensive necessity, you know, stop the bleeding. But they also saw the commercial opportunity.

Jeff If we're going to build this amazing thing.

Emily Let's package it up. Risk would stop being purely a cost center and start becoming a profitable service. They could offer their vast client base.

Jeff Okay, so let's unpack the specific issues, the things that made their old system just unsustainable and kept that revenue opportunity locked away because it wasn't just one thing.

Emily No. There were four core roadblocks threatening their entire roadmap.

Jeff And we can kind of group them.

Emily By can you can group them into two internal operational issues and two external sort of commercial and technical demands. On the internal side, the first big one was just their limited agility.

Jeff Meaning what exactly?

Emily Well, their existing fraud and AML stacks were siloed. They were often separate systems running different databases. And that made it exceptionally difficult for their risk teams to keep pace with new threats.

Jeff So think about what that means in practice.

Emily Yeah. Think about the practical impact. A fraudster finds a new weakness, say exploiting gift card reloads or something with cross-border transactions. It required heavy, time consuming engineering work just to update the rules.

Jeff You're talking weeks, not hours.

Emily Exactly. The time from identifying the threat to deploying the countermeasure was measured in weeks. That's just far too slow.

Jeff And then compounding that problem was the second internal issue, which was this rising compliance and audit pressure.

Emily Ah, yes. As they grew, the regulatory scrutiny grew exponentially.

Jeff It always.

Emily Does. The pressure for fully auditable, transparent processes to reduce regulatory exposure was constant. And their legacy homegrown system, it just didn't provide that granular level of transparency and reporting that regulators demand.

Jeff So it created a huge amount of work for the compliance team.

Emily An enormous operational overhead. And that's a great distinction to make. Compliance is about meeting the rules. Audit pressure is about proving you met the rules reliably, transparently over time. Their system made that second part extremely difficult.

Jeff And the other two points, they really hammer home the technical and the commercial pain.

Emily They do.

Jeff So on the technical front, they had these serious real time high throughput requirements and sixty million transactions a month and growing. You need a decisioning engine that can scale with ultra low latency.

Emily And if you can't make a complex fraud decision in like the blink of an eye, we're talking under one hundred milliseconds. You either halt the transaction which creates friction for the customer, or.

Jeff You let the fraud pass through. And neither of those is sustainable at that scale.

Emily Right. And that technical demand was directly linked to the commercial failure. The fourth roadblock was this massive missed opportunity. No merchant facing FRAML offering.

Jeff They had all this knowledge.

Emily Deep proprietary knowledge about risk, but because their internal system was messy and just wasn't built for external use, they had no way to package it and sell it to their clients. It just constrained their ability to launch a whole new high margin revenue stream.

Jeff That final point is so key for you, the listener. I think no matter your industry, if you have to invest heavily in security or compliance just to run your business, you have to ask yourself, Are we sitting on a strategic asset we aren't selling?

Emily That's the question.

Jeff This payments processor recognized that risk management itself could be repurposed and sold as a product.

Emily And what's so fascinating is that the solution they chose this unified platform. It was designed to address all four challenges at once by, you know, fundamentally transforming the systems architecture.

Jeff So where did they start?

Emily The first essential step was consolidating fraud and AML into a single, unified, end to end, real time platform.

Jeff Which historically were two different worlds.

Emily Totally different silos. Fraud looks backward at a transaction. AML looks forward at suspicious activity, bringing them together instantly. Centralized workflows reduced operational complexity, and just eliminated all that data fragmentation.

Jeff And that unification. That's what set the stage for solving that limited agility problem you mentioned.

Emily It did. They got immediate operational speed by adopting a no code or low code strategy development approach within this new platform.

Jeff Think about the internal power shift there.

Emily It's huge.

Jeff The risk teams, the fraud analysts who live and breathe this stuff, they could suddenly deploy and update rules, logic and models rapidly, right?

Emily Often with just a simple drag and drop interface. And this is the key, without heavy dependence on core engineering teams to write and deploy production code.

Jeff It fundamentally changed the speed of response.

Emily From weeks to hours. It directly addressed that slowness roadblock and to handle the sheer sophistication of modern threats, they also integrated advanced detection methods. They moved way beyond simple rules.

Jeff This is where the machine learning comes in.

Emily Exactly. They adopted what's called ensemble machine learning.

Jeff Okay. So in simple terms what does that mean.

Emily It's about running specialized models that all kind of debate the risk at the same time. They combined supervised learning which finds patterns based on historical fraud data, with unsupervised learning, which is designed to spot anomalies and brand new zero day attacks the system has never seen.

Jeff Like a committee of detectives.

Emily A committee of specialized detectives. Yes, and by running them all at once, they achieved significantly higher accuracy and far fewer false positives. It dramatically improved their proactive detection.

Jeff Okay, so they built a faster, smarter, more unified internal defense system that covers three of the roadblocks. But here's where it gets really strategic.

Emily The revenue engine.

Jeff The revenue engine, the technical architecture that turned this internal solution into a product they could sell. And that was the built in multi-tenancy.

Emily This is the game changer.

Jeff Explain what that means.

Emily Multi-tenancy just means the platform was designed from day one to securely and independently host dozens or hundreds of different clients or tenants, all sharing the core computing infrastructure, but with their data and configurations strictly isolated.

Jeff So it's like a secure, high rise apartment building.

Emily That's a perfect analogy. Every merchant gets their own completely locked down unit. They have customized policies, rules, data storage, but they all share the foundation, the elevators, the maintenance crew, in this case the core processing engine, the ML models, the infrastructure.

Jeff And why is that so critical?

Emily Because maintaining one massive shared system is vastly cheaper and easier than deploying, say, forty separate custom single tenant installations. This built in efficiency is what allowed them to easily package and resell these services to their clients.

Jeff As a white labeled, value added offering.

Emily Exactly. They solved the commercial roadblock by making the underlying technology inherently monetizable.

Jeff So essentially, they took their decade of experience fighting fraud, wrapped it in this secure, scalable tech shell, and then started selling access to it at a profit because their cost to deploy for each new customer was so low.

Emily That's the business model.

Jeff Let's look at the numbers now because the sources show the impact was immediate and tangible. This shift from a slow reactive posture to one built for speed. It generated results that just validated the entire investment.

Emily Well, the first and most crucial result for any payments business was risk reduction. They achieved a massive thirty five percent reduction in fraud losses.

Jeff thirty five percent in a low margin environment, that's millions of dollars.

Emily It translates directly into millions saved on their own book of business instantly and at the same time, their internal agility. That roadblock we talked about, it just skyrocketed much faster. Strategy updates and deploying new fraud countermeasures became ninety eight percent faster, ninety eight percent. So when a new threat emerges, they're deploying a fix instantly. Not weeks later, they're dramatically cutting the window for exposure.

Jeff And the operational efficiency gains are just as staggering. They achieved a four times operational capacity expansion.

Emily Which means the same risk team, the same headcount was able to support this massive increase in volume and the sheer number of new customers buying the service.

Jeff The Titan protection and controlled operating costs at the same time simultaneously. Were the sources clear on how the engineering team handled that? I mean, supporting four times the capacity without hiring more people sounds like a huge lift.

Emily They attribute it directly to the unification by having a single centralized platform for both fraud and AML. All the administrative overhead, the maintenance, the data wrangling, it just dropped precipitously.

Jeff So engineers weren't scrambling to patch separate systems?

Emily No, they were simply updating the core engine. It allowed the team to focus on strategic enhancements, not reactive maintenance.

Jeff And that focus on efficiency. It translated directly into their scaling revenue. The real business story here is just how rapidly they monetized this internal capability. Using that multi-tenancy framework, the platform delivered an incredibly fast time to revenue. The sources confirmed that the new system enabled them to onboard new Subtenants. That is new paying clients in less than one day.

Emily Think about that. Less than a day.

Jeff That implementation speed is just.

Emily It's the secret sauce for monetization. Low friction means fast adoption. If setting up a security service takes months, a client might balk. If it takes less than a day, it's an easy upsell.

Jeff And this capability allowed them to scale incredibly quickly.

Emily To over forty subtenants in a short period. It just confirmed that the incremental revenue stream they envisioned wasn't just realized, it was accelerating rapidly and sustainably.

Jeff So if we synthesize the core lesson here, this case study really illustrates that centralizing risk intelligence, the unified framework system, the real time decisioning, the ensemble ML, that's the necessary technical foundation.

Emily But it's only half the battle.

Jeff It's only half the battle.

Emily The strategic use of multi-tenancy is what truly unlocked the commercial potential. It allowed them to take an internal capability, one they needed for compliance and safety and reposition it as a valuable, scalable and profitable service.

Jeff If they achieve that dual goal.

Emily Exactly tightening internal protection while simultaneously creating this dynamic new stream of income by improving the customer experience.

Jeff This platform, it fundamentally transformed risk management from being purely defensive, just a constant cost strain into a core differentiated business advantage in a super competitive space.

Emily It really.

Jeff Did. So here's our final provocative thought for you to mull over. Considering this payments platform successfully monetized an internal operational capability. Where else in your own industry could a necessary internal cost centre be repurposed?

Emily Right. Think about.

Jeff It. Whether it's supply chain logistics optimization or advanced internal training programs, or maybe even your internal cybersecurity auditing capabilities. Could those be packaged, white labeled, and sold as a differentiated, high margin service to generate revenue?

Emily Look at the internal investments you already make.

Jeff And ask yourself how you might start selling the output of those investments.

Jeff You've been listening to "What the F happened? Fraud and Financial Crime Deconstructed," a DEFEND podcast by Datavisor.

Emily If you want to keep learning between episodes, check out DEFEND Training.

Jeff It's a set of self-paced online courses for fraud and financial crime professionals, practical and built around real world scenarios.

Emily And you can earn CPE credits through the ACFE San Francisco Bay Area chapter.

Jeff You can find it at datavisor.com/defend-training the links in the description.

Emily This episode's audio was generated using Google's Notebook LM based on expert analysis and trusted sources. Thanks for listening. We'll see you next time.