



EPISODE 17 | Analysis

Forrester's Financial Crime Landscape Report

May 4, 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 I want you to think about your morning routine just for a second.

Emily Oh, yeah. Like waking up, maybe grabbing a coffee.

Jeff Right. Exactly. You wake up, you hail a gig economy, ride to the train, maybe swipe through a few profiles on a dating app during the commute.

Emily Phase one.

Jeff Does. Yeah. And then you tap your phone to buy a ridiculously overpriced iced coffee. It all feels, you know, entirely mundane.

Emily Totally normal day, right? Which is wild to think about the infrastructure required simply to allow you to buy that coffee safely.

Jeff We're going to skip the dense corporate jargon and just get straight to the mechanics.

Emily The real nuts and bolts of it.

Jeff Right. And our guide is a freshly released report from Forrester. It's titled The Financial Crime Management Solutions Landscape Q1 twenty twenty six.

Emily It is such a phenomenal look at how financial institutions and actually increasingly completely non-financial companies are. Well, they're weaponizing data to fight back against these sophisticated criminal networks.

Jeff Yeah. Forrester really took a microscope to the actual software vendors supplying this technology. They lay out the exact challenges they're all trying to solve.

Emily Yeah, they really do.

Jeff So we're going to look at how this tech works under the hood. Why regulatory pressures are forcing it into apps you use every single day. And um, how artificial intelligence is just completely rewriting the rules.

Emily It's a whole new ball game now.

Jeff It really is. But to understand the cutting edge, I think we have to start with a massive structural shift that forced or identifies like right at the top of the report. The industry calls it FRAML. That's f r a m l.

Emily Yeah. FRAML And to grasp why FRAML is such a big deal, you really have to look at how businesses historically built their defenses, which was terrible. Right? Oh. Completely inefficient. Forrester defines these financial crime management solutions, or FCMS, as you know, purpose built systems that integrate customer and transactional data. But for decades, the two main pillars of this defense fraud management and anti-money laundering, or AML, they were treated as completely distinct worlds.

Jeff I mean, it's wild to think about the inefficiency of that, the way the old system was structured. It's, um, it's kind of like having a bouncer checking IDs at the front door of a casino.

Emily That's a great way to look at.

Jeff It, right? That's your fraud department there, making sure you are who you say you are, making sure you aren't using a stolen credit card, but then you have an accountant sitting in the back vault watching the cash move around.

Emily And that's the AML side.

Jeff Exactly. Making sure the money isn't tied to a drug cartel or some sanctioned nation. But the crazy part is the bouncer and the accountant are basically locked in separate rooms.

Emily Yeah, they use different software, entirely different vendors, and they just don't share notes.

Jeff But why? Why wouldn't they talk to each other?

Emily Well, they had completely different incentives. Fraud was viewed primarily as a direct financial loss issue for the bank. Like if someone steals your credit card and buys a TV, the bank usually eats that cost, right?

Jeff So they want to stop it just to protect their bottom line.

Emily Exactly. Yeah. But anti-money laundering was viewed strictly as a regulatory compliance issue. The bank isn't necessarily losing its own money when a cartel launders cash through them.

Jeff But if they don't report it.

Emily Right, if they fail to report that activity to the government, they get hit with massive federal fines. So completely different goals led to completely different databases.

Jeff Okay, but Forrester categorizes this as an established market. If it's established, why did it take a multibillion dollar tech arms race to finally force the bouncer and the accountant into the same room? Yeah. I mean, it can't just be that someone suddenly realized sharing data was a cool idea, right?

Emily No, it comes down to the sheer volume of digital transactions today and the evolution of attacker tactics. Specifically something called synthetic identity fraud.

Jeff Oh, wow. What is that?

Emily Well, attackers do not respect corporate silos. Today, a criminal syndicate won't just steal a real person's identity. They will take a real social security number, attach it to a completely fabricated name and birth date, and slowly build up a real credit score over months or even years.

Jeff Wait, really? So they are essentially creating a ghost in the machine?

Emily Exactly a total ghost. And when that synthetic identity opens a bank account, the fraud department's rigid rules might just miss it because, hey, the credit score looks legitimate.

Jeff Ah, so the bouncer lets them in right then.

Emily The criminals use that account to move illicit funds just under the threshold. That would trigger the AML departments alarms. Because the defenses are siloed, the criminals slip right through the gap.

Jeff That is terrifying.

Emily It is. So the shift to framing this converged posture. It fundamentally changes the architecture to catch that.

Jeff How does that actually work in practice, though? What's the mechanism of that shared brain between the two departments?

Emily It starts with the data integration path. Instead of separate databases, the institution feeds all customer interactions into a single unified data lake.

Jeff Okay, so everyone sees everything.

Emily Yeah. And the machine learning weights of the fraud algorithm feed directly into the AML algorithm in real time. So if the fraud module detects slightly anomalous login behavior, say, um, the mouse movements look automated.

Jeff Weight, it can track how your mouse is moving.

Emily Oh, absolutely. It tracks physical cadence, and if it looks like a bot, it doesn't just block the login, it instantly increases the risk score on the AML side.

Jeff Oh that's smart.

Emily Yeah. So when that user tries to wire money an hour later, the AML system is already on high alert. It's an optimized alert framework that sees the entire life cycle of the crime.

Jeff Okay. Which brings up a really critical tension here. Smashing these silos and building unified data lakes sounds great for a bank's security posture, but Forrester lays out how this actually translates into everyday business operations.

Emily Right. The real world impact.

Jeff Exactly. The report identifies three main pillars driving this meeting regulatory requirements, reducing operational costs and improving the customer experience or CX. Let's unpack the regulations first, because they are expanding way beyond Wall Street now.

Emily Oh, way beyond.

Jeff Forrester mentions mandates like Psd2 and etc. what do those actually do?

Emily Well, Psd2 is the Payment Services Directive two in Europe. Among other things, it mandates strong customer authentication. It fundamentally forces payment providers to build highly effective systemic fraud management right into their checkout flows.

Jeff So you can't just ask for a password anymore.

Emily No, you need multifactor verification. And then Nestea is the organization that governs the ACH network. That's the system used for direct deposits and bank transfers in the US.

Jeff Okay. I use that all the time.

Emily We all do. And they have been rolling out incredibly strict rules to crack down on credit, push fraud, where a scammer, you know, tricks you into sending them money directly.

Speaker 3 But the report.

Jeff Shows these AML and know your customer or KYC rules are aggressively bleeding into non-traditional industries too. Like we're talking gaming platforms, gig economy apps, dating sites, and online marketplaces.

Emily Yeah, it's everywhere now.

Jeff Why does a dating app need bank level security software? That seems like overkill.

Emily Well, because a digital platform today is fundamentally a mechanism for exchanging value. And wherever value is exchanged, you have a vector for financial crime. Take a dating app like you mentioned romance scams cost victims billions of dollars annually.

Jeff Oh, wow. Billions.

Emily Billions. If a platform becomes known as a haven for scammers, they lose their user base immediately. Furthermore, if the app offers in-app purchases or subscription gifting. Criminals will use stolen credit cards to buy those virtual goods and then resell the accounts.

Jeff So it becomes a laundering tool.

Emily Exactly. Or look at a gig work app. They have to ensure the driver picking you up is legally authorized to work, and isn't using a synthetic identity to siphon wages or, you know, bypass background checks. The platforms are the new front lines.

Jeff And securing those front lines manually is just economically impossible. Forrester highlights that the labor costs for data scientists and human investigators are skyrocketing right now.

Emily They really are. Like if a marketplace flags ten thousand transactions a day and a human investigator takes three hours to properly review a complex, suspicious activity report. The math just breaks.

Speaker 3 The business.

Jeff Would go bankrupt paying for compliance alone.

Emily Right?

Jeff The sheer scale of global digital transactions requires immense automation. You have to reduce the operational costs of maintaining these complex rules and investigating all those alerts.

Emily But and this is the catch. If you automate too aggressively, you hit the third pillar customer experience. This seems like an incredibly delicate tightrope to walk.

Speaker 3 It is the ultimate tightrope.

Emily Because you have to catch the synthetic identities in the scammers, but you can't annoy your actual customers. Like if I'm out to dinner and I tap to pay and the bank declines my card because their fraud algorithm was a little too sensitive. That is deeply embarrassing.

Speaker 3 It's terrible friction.

Emily Yeah. It's friction.

Jeff And Forrester explicitly notes that customers are highly sensitive to being insulted or subjected to needless friction. The data shows that when there is too much friction, customers don't just call a hotline to complain, right? What do they.

Speaker 3 Do?

Emily They churn. They just delete the dating app. They move their money to a competitor bank.

Jeff Oh wow. So the security teams false positives directly destroy the marketing team's user acquisition.

Emily Precisely. Which means these financial crime management tools aren't just defensive shields anymore. They are core engines of business intelligence. They have to operate invisibly. They are mandated to achieve the highest degree of accuracy with the absolute lowest false positive rates.

Jeff Okay, let's follow that logic. We have a system where human investigators are prohibitively expensive, and false positives actively destroy the customer base. Right. You can't solve that by just throwing more people at the problem. And you can't solve it by just making the old rules stricter. You need a fundamental shift in how the software actually thinks.

Emily Exactly. And according to Forrester, that brings us to the real disruptors. Large language models, AI agents, and decentralized digital identities.

Jeff Yeah. This is where the architecture of financial defense gets incredibly futuristic. Forrester points out that the primary market driver right now is increased regulatory scrutiny colliding with sophisticated attacker tactics. Specifically, they call out deep fakes and advanced scams.

Emily Yeah. To combat this, solutions are heavily leveraging generative AI.

Jeff Because deep fakes are a multi-million dollar liability now, right? Yeah. A criminal can clone a CEO's voice or generate a fake video of someone holding up their ID to bypass a security check. How do legacy systems even begin to handle that?

Emily They don't. They really don't. Heritage systems were entirely rules based. The logic was simple if a transaction is over ten thousand dollars, flag it. If a user logs in from an IP address in a new country, block it. Very rigid, incredibly rigid. Even early machine learning just looked at historical transaction data. But large language models or LLMs, they offer a massive leap in detection capabilities because they can ingest and contextualize wildly larger unstructured data sets.

Jeff But what does that actually look like in the, you know, the two hundred milliseconds of a transaction?

Emily Well, an LLM isn't just looking at the dollar amount and the location. It is analyzing a vast web of behavioral metadata. It looks at the subtle patterns of how you type on your screen, the cadence of your mouse movements, your navigation path through the app, and the entity connections between your account and others.

Jeff So it's looking at the big picture.

Emily Exactly. It understands the context of the behavior, not just the hard numbers.

Jeff Okay. Hold on though. If you have an AI processing all of this multidimensional metadata and it suddenly decides my account needs to be frozen because I don't know, my typing cadence was slightly off. Doesn't the bank have to explain why?

Emily Oh, absolutely.

Jeff Because they can't just walk into a government regulatory meeting, shrug and say, well, the black box told us to do it.

Emily No, they definitely can't. And that is the explainability trap. It is the core vulnerability of the AI era right now. Forrester lists decision explainability right alongside data fragmentation as the primary challenges in this market.

Jeff Because regulators demand a clear lineage of logic.

Emily Exactly. When an institution files a suspicious activity report or SAR to the government, it requires a written narrative detailing the exact evidence of the crime.

Jeff But how does an LLM write a legal narrative based on vector data? Like how does it explain a mouse click cadence in a legal document?

Emily That's where AI comes in. Vendors are deploying AI agents to act as co-pilots for human investigators. The AI triages the alert pulls the multi-dimensional data and actually drafts the SA narrative, translating its complex algorithmic decision into a human readable explanation.

Jeff Oh, so it translates itself, right?

Emily And then the human reviews, it tweaks it and files it. The AI must remain explainable to prevent compliance violations and to quickly resolve customer disputes without adding friction.

Jeff That's fascinating. Now, you also mentioned data fragmentation. Forrester points to decentralized digital identities, or dIDs, as the disruptor. Solving this. What exactly is a D ID and how does it fix the fragmentation problem?

Emily Think about the current KYC process. Every time you sign up for a crypto exchange, a gig app, or a new bank, you take a photo of your physical driver's license and you upload it.

Jeff Right, which feels super sketchy.

Emily Sometimes it is because you're highly sensitive. Identity data is now fragmented across dozens of corporate servers globally, creating a massive surface area for hackers to steal.

Jeff And that's a gold mine for anyone wanting to build those synthetic identities we talked about earlier.

Emily Precisely. It's a feedback loop of fraud, but D IDs represent a shift toward government issued, cryptographically secure digital credentials. Instead of uploading a Jpeg of your passport to a server, your identity lives in a secure digital wallet on your device.

Jeff Okay, so it stays with me.

Emily Yes. When an app needs to verify you are over eighteen or that you are a citizen, you don't give them your data. You use cryptographic technology like a zero knowledge proof to verify the claim is true without revealing the underlying information.

Jeff Oh that's incredible.

Emily Yeah, the app gets a cryptographic guarantee of your identity verified by a trusted network, but they don't have to store your sensitive documents. It digitizes trust and eliminates the fragmented honeypots of data.

Jeff Okay, so if I'm a business leader trying to defend my platform against deepfakes, and I know I need this LLM driven anomaly detection and D ID integration, I am absolutely not building this infrastructure from scratch in my IT department.

Emily No. Definitely not. You'd be crazy to try.

Jeff Right. I have to buy it. And this is where Forrester provides a roadmap of the actual battlefield. They reviewed forty two different vendors operating in this space right now.

Emily It is a sprawling market. Forrester categorizes the forty two vendors by revenue size to help buyers kind of orient themselves. You have the large vendors generating over two hundred and fifty million dollars annually.

Jeff But you know, if I'm the CTO of a new online marketplace, I don't really care about the vendors revenue tier. I care about what their software actually does naturally. And Forrester breaks this down into a highly strategic matrix of core use cases versus extended use cases.

Emily And that is exactly how buyers have to approach it. The core use cases are the foundational elements everyone needs just to play the game. Risk scoring model management, alert queues, operational reporting, and most importantly, data integration.

Jeff Let's talk about data integration for a second, because from an engineering standpoint, that sounds like an absolute nightmare.

Emily Oh, it is arguably the biggest hurdle. Imagine a regional bank running on a legacy mainframe banking core built in the nineteen nineties.

Jeff Oh, yikes.

Emily By taking that siloed, archaic data at standardizing it, normalizing it, and piping it into a modern AI platform in real time without breaking the bank's operations, that is an incredibly heavy lift. A vendor that excels at core data integration is highly valuable to those legacy institutions.

Jeff But if everyone has the core features, then the extended use cases are where the battle for differentiation actually happens.

Emily Yes, that's where they stand out.

Jeff This is where you see functionalities like customer screening. So that means checking databases for politically exposed persons or RFPs, and actively scanning global adverse media to see if, say, a new client was recently indicted for embezzlement somewhere in the world.

Emily Exactly. And there's also deep transaction monitoring. This is specifically designed to catch things like structuring.

Jeff Structuring.

Emily Yeah. That's where a sophisticated money launderer breaks up large amounts of cash into tiny, erratic deposits over time just to avoid setting off those static reporting thresholds.

Jeff Oh, clever. The report also lists integration with third party SIM. What is SIM?

Emily That's customer identity and access management. It's the system that controls how users securely log in, manage their passwords, and authenticate their sessions.

Jeff Okay. Makes sense.

Emily And if a vendor can natively integrate their fraud detection into the SIM flow, they can stop an account takeover. The second a hacker tries to log in, rather than waiting for them to actually initiate a fraudulent transaction.

Jeff Oh, so you stop it at the front door. Forrester notes that omnichannel fit is rapidly becoming table stakes, meaning the software has to protect the mobile app, the website, the call center, and the physical branch. Equally, it.

Emily Has to be everywhere.

Jeff So if you are that CTO staring at a list of forty two vendors, and they all claim to use AI, and they all claim to be omnichannel, how do you actually choose?

Emily Well, you map the vendor specific differentiation to your unique behavioral vulnerabilities. It's really about finding the exact puzzle piece for your business. First, you look at geographic focus. Does

the vendor understand the specific data privacy regulations of the European Union versus North America? Right. Do they offer jurisdiction specific policy packs right out of the box?

Jeff So you don't have to hire an army of lawyers to manually configure the rules for every new country you expand into?

Emily Exactly. Then there's industry focus. The fraud patterns of a cryptocurrency exchange look fundamentally different from the fraud patterns of a local retail bank.

Jeff That makes total sense.

Emily And finally, you evaluate those extended use cases. Forrester highlights vendors like DataVisor as being heavily focused on digital fraud management, which is perfect for a platform worried about account takeovers? Other vendors might offer a broader, heavier blanket of compliance reporting for traditional banks.

Jeff So you aren't just buying software, you're buying the algorithmic model that best understands how your specific users behave.

Emily Exactly.

Jeff So there really is no one size fits all magic bullet. It's a completely bespoke defense system tailored to the unique attack surface of the business, designed to catch the anomaly without ruining the experience. For the ninety nine percent of legitimate users.

Emily It is a remarkable balancing act of heavy regulation, cutting edge AI, and consumer psychology.

Jeff It really reframes how you look at the digital world. I mean, we started today by looking at the merging of the bouncer and the accountant, how the traditional silos of fraud and AML are collapsing into this massive Converged framework architecture.

Emily Yeah, that's the foundation of all of this.

Jeff And we unpacked how the expansion of digital value forced this bank grade security out of Wall Street and into the gig work and dating apps we use daily.

Emily We examine the mechanics of the technological shift to where large language models are analyzing behavioral metadata to catch synthetic identities, and agentic AI is drafting human readable legal narratives to ensure those decisions remain explainable to regulators.

Jeff Right. And we mapped the strategic battlefield of the forty two vendors fighting to provide the perfect mix of legacy data integration and specialized extended defenses like cryptographic digital identities. It really is a multi-million dollar invisible shield, keeping the global financial system functioning at millisecond speeds.

Emily It truly is.

Jeff But before we wrap up, I want to leave you with a final thought to ponder something that builds on where this technology is inevitably heading.

Emily Yeah, because the implications of decentralized digital identities go far beyond just logging into a bank.

Jeff They really do. Forrester highlighted dd id as a top disruptor meant to solve the fragmentation of our personal data. But if in the very near future, your ability to bank to date, to catch a ride, or to get a gig economy job relies on a single, immutable digital identity.

Emily A single source of truth.

Jeff Right? One that is seamlessly and constantly being scored by invisible AI agents across a global network. Well, who ultimately controls the keys to your digital reputation?

Emily That's the big question.

Jeff And more importantly, if the multi-dimensional AI model hallucinates or just gets the context wrong, how do you prove your innocence to a machine?

Emily It is the ultimate double edged sword. We are building frictionless security, but the cost might be an invisible, unappealable algorithmic judgment.

Jeff Yeah. So next time you're standing in line, tapping your phone for that morning iced coffee, think about the unseen war being fought in the milliseconds before approved flashes on the screen. Thank you for joining us on this deep dive. Keep learning, keep questioning, and never stop exploring the hidden systems that power your daily life.

Jeff You've been listening to "What the F Happened? Fraud and Financial Crime Deconstructed," a DEFEND podcast by DataVisor. If you want to keep learning between episodes, check out DEFEND Training, 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. You can find it at datavisor.com/defend-training. The link is in the description.

Jeff 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.