EPISODE 1 | Monthly Brief

January 2026 Fraud & Financial Crime Trends

JANUARY 12, 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.

Emily Welcome to the deep dive. You know, when it comes to financial crime, defense, the landscape, it isn't just shifting anymore. It's, um, it's experiencing what I can only call a full on regulatory driven technological revolution. We're really moving away from that old mindset of just, you know, accepting loss prevention. We're moving toward a proactive and mandatory real time defense strategy. So today, we've taken a deep breath and plunged into a whole stack of specialized sources. We're talking research reports, technical analyses, all detailing these critical fraud trends and, crucially, the binding regulatory deadlines that are taking effect in early twenty twenty six. Our mission is to give you a shortcut, really, to understanding the three big imperatives facing financial institutions right now. First, these dramatic new liability rules for how many moves. Second, the new attack surfaces that open banking introduces, and third, how AI driven platforms are being used for defense. Turning risk management from a cost center into, well, a potential source of revenue.

Jeff It really is an inflection point. Absolutely. What's genuinely fascinating here is just how quickly the whole operational conversation has changed. It's no longer about if you need better defenses, right. It's about how fast you can modernize your core systems to meet all these challenges at once. We saw this captured perfectly by Datavisor CEO Tony Chu. He basically said, the more proactive we can become, the better protected institutions and their members will be. That's where fraud prevention is headed.

Emily So proactivity isn't just a best practice.

Jeff Not anymore. And now it's a regulatory necessity that I mean it starts this quarter.

Emily Okay. Let's start with the biggest one. Then the, uh, the regulatory tidal wave impacting money movement. The new rules from Nacha governing the ACH network were already in January twenty twenty six. And the compliance deadline for this new framework is March twentieth. That means implementation needs to be finalized. Like right now.

Jeff This is the tectonic shift you mentioned. It really is. For years, ACH fraud detection focused well, almost entirely on unauthorized debit.

Emily Someone pulling money out of your account without permission.

Jeff Exactly. That was the standard threat model. The game changer is that the liability rules now explicitly expand to include credit push fraud.

Emily So credit push, just to be clear, that means the user or I guess in a lot of these cases, the business, they're the ones actually initiating the transfer. Precisely. But they've been tricked into doing it.

Jeff Tricked is the right word. We're talking specifically about these, uh, really sophisticated social engineering schemes, things like business email compromise bec where a CFO is impersonated. Right. Or these elaborate vendor impersonation schemes where someone changes the bank account on file. The funds were authorized by the account holder, but under fraudulent pretenses.

Emily And that's so much harder to detect than just a simple unauthorized debit.

Jeff How much harder?

Emily And the regulatory consequence now is that the liability for catching the scam shifts from the receiving bank to the sender.

Jeff It does.

Emily That completely flips the traditional fraud defense model.

Jeff It absolutely does. The responsibility for detection moves squarely to the center. So the office, the originating depository, financial institutions and other big non-consumer originators. And this is significant because traditionally the OFI just saw its job as verifying the originators intent, not necessarily the legitimacy of the account on the other end.

Emily But now they have to.

Jeff Now they must implement these robust risk based controls. They have to monitor ACH files and batches in real time or something very close to it before that money leaves their institution. The mandate is basically forcing them to build these sophisticated behavioral and identity models that honestly, they just didn't need before for ACH.

Emily That feels like a provocative alignment. I mean, if the US is pushing sender side accountability, how does this actually compare globally? Is this an alignment or are we just playing catch up?

Jeff It's definitely an alignment. But yeah, maybe playing catch up. In a sense, this change in the US explicitly mirrors the shift toward what's called authorized push payment or app fraud trends. We've been seeing this in the UK and the EU for several years now. When app fraud exploded over there, regulators moved quickly. They mandated that the responsibility, the due diligence had to fall on the institution that was initiating the push payment. So this is a very clear signal sender side accountability for stopping fraudulent money. Movement is, well, it's quickly becoming the global standard. If you're a global Fi, you already know this standard. Now US domestic payments have to conform.

Emily Okay. So Nacha is demanding accountability for the money leaving the system. At the same time, the CFPB is demanding accountability for the data that's fueling that movement. Let's get into the other huge shift that kicked off this January the Cfpb's open Banking rule, section six thirty three, right.

Jeff This rule is the official catalyst. It's what's modernizing secure data access across the whole US financial ecosystem. And we know the deadline structure, the large banks.

Emily Those with over two hundred and fifty billion dollars in assets.

Jeff That's them. They have to comply by April twenty twenty six. The mandate requires them to provide secure API access to consumer financial data whenever the consumer authorizes it.

Emily And this isn't just a new rule. It's a it's a technical mandate for transformation, right. What older methods are these APIs replacing?

Jeff They're explicitly replacing traditional screen scraping for years, third party apps, you know, budgeting tools, financial advisers, they would log in using a consumer's own credentials and just scrape the data off the website interface.

Emily Which sounds so clunky and insecure.

Jeff It was, and it gave the third party way too much access. The CFPB rule mandates standardized API interfaces that only allow secure transmission of very specific data points. It standardizes the process, it improves security, and it's going to dramatically accelerate US open banking adoption.

Emily But with all accelerated innovation, it opens up new attack surfaces. It has to.

Jeff Which brings us right to the next phase of this deep dive the new fraud vectors. I mean, the speed and convenience of these APIs are great for innovation, but they have to be just incredibly tempting targets for organized crime. They're a massive target. Yes. Our sources are really clear on this. While the standardized APIs enable secure data movement, that standardization itself can be exploited. We're talking sophisticated high velocity attacks, synthetic identity fraud, account takeover, especially if the API controls are weak.

Emily It's an inherent side effect.

Jeff Then it is if you build a faster, standardized door, well, sophisticated criminals will find a way to test the lock on that door faster.

Emily So if open banking means thousands of third parties might need real time data access through an API, how do fraud teams make sure the entity making that request is the real account holder, and not some attacker? Using a cleverly crafted synthetic ID that passes the basic checks. This seems like the core conflict between compliance and security.

Jeff And this is where the concept of identity orchestration becomes, well, not just important, but absolutely fundamental. It has to be the top priority for these teams after the CFPB deadlines. Identity orchestration is the discipline of validating the real person behind any request an API pull an account, opening a payment without adding a bunch of friction for legitimate users.

Emily Can you break that down? What does that orchestration look like in practice? What pieces are being orchestrated?

Jeff Think of it like a dynamic security assembly line. So instead of relying on one single check like just a password or an IP address, orchestration dynamically links multiple signals in real time Things like device intelligence, geolocation, behavioral biometrics, and the transaction context itself. For example, if an API request comes from a device that normally logs in from California, but maybe the behavioral patterns look unusual and the IP is masked. The orchestration layer automatically triggers a high friction challenge. The goal is to enforce the security the CFPB rules require, while making sure that, you know, ninety nine percent of legitimate users have a completely seamless experience. That balancing act is the core challenge.

Emily That transition from regulatory pressure and new risks. It brings us right to the technological response that's needed. We're talking about unifying fraud and anti-money laundering into what the industry now calls framework, empowering it with real time AI.

Jeff Exactly. We have to stop thinking of fraud and AML as these separate, siloed cost centers. Historically, they were separate because, well, fraud was a fast retail problem and AML was a slow regulatory compliance problem.

Emily But the data they use is largely the same.

Jeff It's largely the same customer entity transaction flow, network relationships. Unifying them is how leaders are going to move faster, operate more efficiently, and, crucially, operationalize their defense for growth.

Emily That idea of turning risk into revenue sounds a little counterintuitive, but the case study we looked at on the payments processor illustrates this perfectly. They modernized their whole risk operation using this real time framework decisioning. What were the tangible results?

Jeff The results were truly transformational. They really show the power of operationalizing defense. This payments processor, they achieved a thirty five percent reduction in fraud losses.

Emily Which is huge.

Jeff It's substantial. And they did that all while scaling to support over sixty million monthly transactions. So they didn't just save money. They stabilized their whole platform to handle immense growth without buckling under the risk.

Emily But when you're dealing with that kind of volume, that kind of real time attack, the speed of your strategy updates is just vital. You can't wait three weeks for an IT cycle if an attack pattern changes.

Jeff Exactly. And that's where the tech really shown. They achieved this massive leap in agility. Their fraud strategy updates became ninety eight percent faster, ninety percent, ninety eight percent. And they did this by using ensemble machine learning. And this is key. No. And low code platforms, I mean ninety eight percent faster is the difference between updating your defense system in an afternoon versus running a three month waterfall project. It means you can react to a new attack vector launched by a criminals AI in real time. That's the definition of proactive defense.

Emily Okay, let's pivot back to that idea of turning risk into revenue. How did this processor actually convert their internal defense system into an external product?

Jeff It all came down to architecture, specifically building the platform with multi-tenancy in mind from day one.

Emily Meaning it can host multiple clients at once.

Jeff Right? It can securely host and manage risk ops for multiple separate clients simultaneously. And because their system was so agile and so robust, they're able to quickly white label their fraud and AML offering. Our sources note they scaled up to over forty subtenants in a single day.

Emily Wow.

Jeff This is the ultimate competitive advantage. They took their core operational expense risk management and packaged it as a marketable product. They created a powerful new revenue stream.

Emily That really is the power of unified, real time friemel in action. But even the best AI needs human oversight. When you're managing sixty million transactions a month, investigators can get overwhelmed by alerts. So we need to talk about the tech that makes the human investigator faster. AI Alert Summary.

Jeff This is direct answer to investigator burnout and inefficiency. I mean, managing thousands of high velocity alerts every day is just overwhelming. If the investigator has to manually pull data from four different systems just to understand the context, the solution being deployed now is this AI alert summary button. An investigator just clicks it, and the AI instantly synthesizes all the associated data into one digestible window.

Emily What specifically is in that automated summary that wasn't immediately available before.

Jeff Well, before an investigator might open an alert and just see a rule trigger. Yeah. Then they'd have to manually check case management history, look up the entities behavioral score, review notes from previous reviews.

Emily All that legwork.

Jeff All that legwork. The AI summary eliminates it. It delivers comprehensive context. The precise reason the alert was triggered, all the key risk indicators highlighted. And it pulls data from every silo. Rules review history. Investigator notes, entity details.

Emily So the benefit isn't just about being faster, it's about context and the quality of the decision.

Jeff Absolutely. The practical impact is huge. It drastically cuts the time needed to understand the core issue, which boosts investigator efficiency by a massive margin, but more importantly, because it instantly delivers that history and specific risk indicators, it leads to much more informed and accurate decisions. You're not just making them faster, you're making them with one hundred percent of the relevant data right there.

Emily Okay, shifting gears a bit, moving from traditional payment rails and AI. Let's look forward to the next frontier. The challenges and opportunities with emerging payment methods, specifically stablecoins, right?

Jeff Stablecoins and digital assets are often seen by legacy fraud teams as a kind of financial crime blind spot, a place where illicit activity can hide. Because of this perceived anonymity.

Emily But her source material makes this really fascinating, counterintuitive claim that stablecoins, even though they operate on decentralized ledgers, might actually be easier to monitor than cash or even traditional wires. Why is that?

Jeff It all comes down to on chain visibility. When you send a wire, your bank sees your ID and the other person's ID, but the underlying history of those funds is totally opaque. With stablecoin transactions, because they happen on public, immutable blockchains, that on chain visibility is permanent. And when you pair that data with modern analytics platforms, fraud and AML teams can detect risk earlier and trace illicit activity way faster.

Emily So the very transparency of the blockchain, which can feel really intimidating and technical, is actually a defensive advantage over these opaque traditional banking rails.

Jeff Precisely the transparency of on chain data can reveal entire patterns of activity. Wallets interacting, the velocity of transfers, network size, things that are simply invisible in traditional rails like card or ACH. And what the sources show is that where fraud still succeeds in the crypto space, it's usually exploiting operational gaps at the on ramps and off ramps.

Emily Like at exchanges.

Jeff Exactly. Gaps in KYC, AML at exchanges, not the anonymity of the tech itself. So the core defense relies on knowing how to use those crypto native signals to strengthen your overall defense strategy. As stablecoin usage expands, you're turning decentralization into a defensive edge.

Emily That shifts the focus dramatically. The threat isn't the technology's inherent risk. It's the organization's preparation, its capacity to integrate those crypto native signals into their existing framework platform. This has been a whirlwind of a deep dive into twenty twenty six. We've really covered the three pillars that have to be addressed the dramatic regulatory shift towards sender accountability with Nacha, the mandatory secure data sharing via the CFPB, and the resulting need for sophisticated identity orchestration. And of course, the essential tech solution of unifying fraud and AML with real time AI.

Jeff The summary is really unequivocal. The defense game for the next few years is all about speed, unification and real time decisioning. AI isn't an optional add on anymore. It's becoming the core engine for detection, for supporting high velocity payments, and for driving the adoption of these unified fraud plus AML platforms. If you aren't moving toward real time decisioning and unification, you are falling behind.

Emily It really seems like that unified platform is quickly becoming the new industry standard for efficiency and frankly, for a competitive advantage.

Jeff It is. So here is the final thought for you to consider. And this pulls from the broader challenges outlined in the twenty twenty six Fraud Trends research. If unified fraud and AML is now the standard for operating efficiently at scale. How prepared are your current systems, your processes, and your people to face the five specific operational challenges that teams confront when they try to genuinely operationalize AI at scale?

Emily It's not just about buying the AI models.

Jeff Not at all. It's about having the governance, the data infrastructure, the investigator training, and that low code agility. You need to make that technology a revenue generating reality within your existing complex framework. That operational hurdle that's often the silent killer of even the best modernization efforts.

Emily You've been listening to “What the F Happened? Fraud and Financial Crime Deconstructed”, a DEFEND podcast by Datavisor.

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.