EPISODE 9 | Monthly Brief

March 2026 Fraud & Financial Crime Trends

MARCH 9, 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 today's deep dive. If you are joining us right now, you are the learner. Absolutely. And maybe you're an industry professional gearing up for a, you know, a really high stakes compliance meeting or catching up on the latest regulatory shifts.

Jeff Or maybe you're just an insanely curious mind, right?

Emily A curious mind wanting to understand the hidden high speed mechanics keeping your money safe in 2026. Either way, you are in the exact right place.

Jeff You really.

Emily Are. Our mission today is to decode the massive systemic shifts happening right now across financial crime, fraud prevention, and banking regulations.

Jeff It's a lot of ground to cover.

Emily It is. And to do that, we are tearing into a massive stack of research today, specifically anchored by the March 2026 DataVisor DEFEND material.

Jeff Which is just a gold mine of information.

Emily A total treasure trove. It includes a wealth of regulatory updates, real world case studies, and AI tech developments that fundamentally change how we think about financial security.

Jeff And we should probably start with the overarching theme here.

Emily Yes, to kick us off, there is a really powerful quote in this research from Brian Hughes.

Jeff Oh, that's a great one, right?

Emily He's the president of Brian Hughes Consulting and a board director at Affirm. And he says, and I quote, you can't wait for the losses to show up. Actively benchmark yourself and point out your flaws before the fraudsters find them.

Jeff That quote is, uh, honestly, it's the absolute perfect lens for today's discussion.

Emily How so?

Jeff Because it completely encapsulates the grand pivot the entire financial industry is desperately trying to execute right now.

Emily The shift away from being reactive.

Jeff Exactly. We are moving away from a historically reactive world. I mean, for decades, the standard operating procedure was basically defensive. You wait for an alert to trigger.

Emily Or wait for a customer to call in a total panic about missing funds.

Jeff Right? Which is even worse. Wait. And then you scramble to investigate. But we are now being forced into a proactive posture. You have to use artificial intelligence and real time data to stop the fraud before the transaction even completes.

Emily Because the money moves too fast. Now.

Jeff Far too fast. The losses are instant, and the bad actors are far too sophisticated to simply play catch up anymore.

Emily Okay, let's unpack this. I want to start with what we're looking at as the 2026 regulatory tsunami.

Jeff It really is a tsunami.

Emily The research highlights three major regulatory shifts happening right now. And the first one is the CFPB rule ten thirty three.

Jeff Are open banking.

Emily Yes. Open banking. The implementation phases are kicking off this year in 2026 starting with the largest institutions.

Jeff Which is going to be a heavy lift.

Emily Huge lift. The core fact here is that it requires secure consumer authorized access to account data through standardized APIs.

Jeff Ultimately replacing the legacy practice of screen scraping.

Emily Right? And for anyone who needs a quick visual on what that means, I like to compare old school screen scraping to handing a complete stranger the physical keys to your house.

Jeff That's a scary thought.

Emily Just so they can go inside and check what's in your fridge. You literally give a third party app your actual bank username and password, and they have total unrestricted access to your digital life.

Jeff It was always a security nightmare.

Emily Totally. So the new API rule is like giving them a temporary, highly restricted guest pass. They only get to see the fridge and you never hand over your master keys.

Jeff It is a massive upgrade for consumer security, certainly, but and this is crucial, there is a very critical hidden catch here for the financial institutions themselves.

Emily Okay. What is.

Jeff It? It comes down to monitoring blind spots. When banks move away from that old screen scraping model to API based access, they're going to lose a lot of traditional login and session signals.

Emily What kind of signals are we talking about exactly?

Jeff Like the IP address, the specific device type, or even the browser fingerprint of this scraping bot or service that's logging in?

Emily Oh, because they aren't logging in through a browser anymore?

Jeff Exactly. Banks used to rely on those breadcrumbs to spot suspicious activity with API's. That telemetry vanishes or changes fundamentally because the connection is happening server to server.

Emily So the bank is essentially blind to the device?

Jeff Basically, yes. So banks must now rely on much stronger behavioral monitoring of the API activity itself to detect anomalies.

Emily That makes sense.

Jeff Furthermore, because consumer financial data is becoming highly portable, meaning you can share your verified account histories across multiple platforms instantly, it completely rewrites how institutions handle identity verification and onboarding risk.

Emily Right. Because if I can just port my entire financial history over to a new app with a single click, that new app has to trust the data. Yes, but they also have to verify I'm the one actually clicking the button, not some fraudster who intercepted my session.

Jeff Precisely. And the rules note that while institutions absolutely have the right to deny data access, if they detect fraud or security risks.

Emily They can't just do it arbitrarily.

Jeff Exactly. You can't just block a competitor's app and claim it was a security risk without the data trails to back it up. Those denials must be rigorously documented and purely risk based.

Emily The governance around those access decisions is going to be under a massive microscope.

Jeff It is. Which leads perfectly into the second major regulatory update. This one is from FinCEN regarding beneficial ownership.

Emily Yes, the FinCEN beneficial ownership relief. So FinCEN recently issued an order that provides relief from the CDC rule. That's customer due diligence, right? Specifically, it provides relief from the requirement to identify and verify beneficial ownership every single time an existing legal entity customer opens a new account.

Jeff Which sounds like a good thing on paper.

Emily Well, yeah, if a business already banks with you and they decide to open a new checking account, you don't have to put them through the wringer again with stacks of paperwork to prove exactly who owns the company.

Jeff Assuming you have no reason to doubt the data you already have on file, right?

Emily Assuming that so from a customer experience standpoint, that sounds fantastic. Less friction, less annoying paperwork. Honestly, my immediate reaction is that this sounds incredibly risky. If you aren't checking their ID every time they open a new account, aren't you just leaving the back door wide open for a fraudster who might have quietly bought out a legitimate business?

Jeff That is exactly the friction point here. What's fascinating here is the immediate trade off. It sounds like relaxation of the rules, but what it actually does is place a massive crushing pressure on an institution's ongoing monitoring capabilities.

Emily Because you aren't checking at the door.

Jeff Exactly. If you aren't checking their ID at the door every single time they walk into a new room, your internal cameras, meaning your ongoing due diligence processes had better be completely flawless.

Emily So the bank basically has to spot the behavioral changes organically.

Jeff Precisely. You have to catch when ownership information changes organically based on how the account is behaving. Wow. The relief explicitly states you can rely on past data only until you become aware of facts that call its reliability into question.

Emily So your risk based reviews have to be razor sharp.

Jeff They do. You have to detect those subtle indicators, maybe a sudden shift in wire transfer destinations, or a change in the authorized signers that warrant refreshing that beneficial ownership data outside of the standard account opening process.

Emily And you have to document all of this. Institutions have to maintain clear files showing exactly how their ongoing monitoring supports the accuracy of that info. It's a lot of plates to keep spinning.

Jeff It really is. And that brings us to the third piece of this regulatory puzzle. The OCC updated their bsam examination procedures.

Emily The Bank Secrecy Act and anti-money laundering protocols.

Jeff Exactly as of February first, 2026. The OCC updated these procedures specifically for community banks. It shifts heavily toward a risk based exam approach rather than a rigid, one size fits all testing model.

Emily If we synthesize these three regulatory updates, a very clear picture emerges, which is whether it's the CFPB dealing with API's. FinCEN easing up on redundant CTD paperwork or the OCC looking at community banks. The era of checking a static compliance box is officially over.

Jeff It's done.

Emily Examiners are now going to focus heavily on an institution's specific, unique, high risk areas, whether that's certain customer segments, specific products, or unusual transaction patterns.

Jeff Meaning a community bank in rural Iowa is going to be tested very differently than a regional bank in Miami handling heavy international wires.

Emily Precisely. They're also going to rely far more on the bank's own independent testing.

Jeff Okay, so what does that mean in practice? It means you can no longer buy an off the shelf monitoring system, plug it in, and assume you are compliant just because the software is running right. Institutions must prove definitively that their transaction monitoring aligns specifically with their unique risk profile, and that it is genuinely effective at catching suspicious activity.

Emily Okay, but let's be real for a second. Proving that your custom monitoring actually works sounds great in a regulatory briefing. Sure, but how does an institution actually pull that off without drowning their staff in false alarms? Because the DataVisor research provides a real world case study here.

Jeff Yes, the attack spotlight.

Emily Here's where it gets really interesting. It's an attack spotlight on a large North American credit union that completely transformed its approach. They shifted from legacy, alert driven workflows to proactive, context aware risk scoring across everything onboarding, login and money movement.

Jeff And the results they achieved are exactly why the industry is moving away from those off the shelf rules based systems.

Emily The numbers are absolutely staggering. Let's actually visualize what this means for the people doing the work before this shift. They're fraud. Analysts were drowning in about three thousand manual reviews per day.

Jeff Three thousand.

Emily Imagine that you sit at your desk, you have eight hours, and there are thousands of alerts blinking red. You are basically a human rubber stamp. Clicking approve or deny until your eyes blur. Just trying to clear the queue.

Jeff It's totally unsustainable.

Emily But by implementing real time behavior based risk detection, they achieved a ninety eight percent reduction in manual reviews.

Jeff Incredible.

Emily They dropped from three thousand down to fewer than seventy per day.

Jeff That is a fundamental paradigm shift. When you drop your manual reviews that drastically, you aren't just saving time. You are completely repurposing your human intelligence. You're freeing up highly trained human analysts to focus on complex, nuanced investigations. It allows the human experts to look for the invisible threads connecting organized fraud rings, rather than just drowning in a sea of false positives generated by a legacy system.

Emily They also saw a ninety percent reduction in member friction.

Jeff Which the customers love.

Emily Exactly. Meaning things like stepping up authentication with a one time password and OTP were only applied when the risk signals actually justified it. You aren't annoying every single customer who tries to transfer fifty bucks to their kid.

Jeff And the payoff was immediate.

Emily There's this incredible moment in the case study, they were able to deploy a new rule. The exact same night, a new fraud pattern was identified, and it instantly prevented an additional 20000 dollars in losses.

Jeff The same night.

Emily Boom. Same night. Twenty grand.

Jeff Save that speed is the critical factor. But according to the latest industry data in this research, most of the industry isn't moving anywhere near that fast.

Emily No they're not.

Jeff They call it the AI readiness gap. The report shows that seventy four percent of fraud and AML leaders see AI driven fraud like deepfakes, synthetic identities, coordinated fraud rings as a top threat right now.

Emily Which makes sense.

Jeff But here is the terrifying part. Sixty seven percent admit their organizations lack the infrastructure to actually deploy effective AI defenses against it.

Emily I want to push back on that a bit, though. If sixty seven percent lack the infrastructure, isn't that just a symptom of the fact that ripping out legacy banking technology takes years and costs millions of dollars.

Jeff It certainly does.

Emily You can't just flip a switch and suddenly have Google level AI in a regional credit union.

Jeff You're right to point out the operational hurdle. But I want you to consider the asymmetrical arms race unfolding here.

Emily Okay.

Jeff Fraudsters do not have legacy IT infrastructure holding them back. They do not have procurement cycles or compliance committees.

Emily They're just moving fast and breaking things.

Jeff Exactly. They are utilizing generative AI and machine learning to evolve their attack vectors at blistering speeds. If a financial institution is trying to fight AI speed attacks using human speed legacy batch processing systems, they are already losing.

Emily The math simply doesn't work.

Jeff The math does not work in their favor at all. This infrastructural bottleneck is exactly why eighty one percent of organizations are now actively moving toward unified fraud and AML strategies.

Emily Because you can't be siloed anymore.

Jeff You cannot have your fraud team and your AML team operating in separate silos. When the AI tools attacking them are unified.

Emily Well, the research outlines a pretty wild solution called the five minute fraud strategy. It's powered by data visors feature engine. Yes, this is essentially an AI copilot and a no code or low code studio that takes messy multi-source data and turns it into real time risk signals.

Jeff And the pitch here is that you don't need to know Java, right? You don't need Python. You don't need to submit a ticket to your engineering team and wait three weeks for a new rule.

Emily The democratization of feature engineering is arguably the most important technical leap in fraud prevention right now.

Jeff It really is.

Emily Okay, let's pause there. For our listeners who aren't data scientists, what exactly do we mean by feature engineering?

Jeff Great question. In machine learning, a feature is basically a specific clue or data point the AI looks at to make a decision.

Emily Give me an example, for example.

Jeff How many times did this specific user change their password and then immediately add a new payee within the last hour? Got it. That complex sequence of events is a feature in the past defining that clue, extracting the data, and coding it into the system so the AI could understand. It took weeks of intensive coding by specialized engineers.

Emily And now, an analyst can use plain language AI generation.

Jeff Which is mind blowing.

Emily You can literally just type a prompt like flag cards with three or more high risk merchants in 24 hours, and the AI agent instantly generates a production ready feature.

Jeff Complete with debugging and optimization suggestions.

Emily It's wild. It comes out of the box with hundreds of pre-built features for account takeover, ACH fraud, mule networks, promo abuse.

Jeff The ease of creation is vital, but the operational performance is what makes it viable for enterprise banking.

Emily Let's talk about the specs.

Jeff Let's look at the technical specifications. It processes over fifteen thousand queries per second with a feature computation time of under one hundred milliseconds.

Emily Let's ground that for a second one hundred milliseconds.

Jeff That's fast.

Emily To put that in perspective, the literal blink of a human eye takes about three hundred milliseconds. So before you can even blink, the AI has pulled data from multiple sources, checked your behavioral history, and decided if your transaction is safe.

Jeff Exactly. If we connect this to the bigger picture, that sub one hundred millisecond latency is the holy grail for institutions.

Emily Because it doesn't slow down the user.

Jeff zero added latency to the customer experience. Decisions are being calculated and executed. Live in the micro-moments between a user clicking submit and the money actually leaving the account.

Emily Wow.

Jeff Furthermore, the architecture allows you to define a feature once and immediately deploy it across standard rules. Supervised machine learning models and unsupervised machine learning, or UML.

Emily And just for clarity. Unsupervised machine learning UML is when the AI looks at raw data and finds hidden patterns or anomalies on its own without being explicitly told what fraud looks like beforehand. Right, so you're catching the unknown threats, not just the ones you already know about.

Jeff Precisely. No duplicated work. Completely consistent logic across the entire platform. Whether you are running simple rules or advanced UML.

Emily That speed and consistency are going to be non-negotiable as we look ahead at the rest of 2026.

Jeff Absolutely non-negotiable.

Emily The research points out that the upcoming Nacha 2026 rules are expanding explicit fraud monitoring requirements for both ACH credits and debits. Huge shift institutions are going to have to detect scams, account takeovers and mule activity in real time. DataVisor actually put together a whole Nacha 2026 readiness Kit to evaluate governance.

Jeff Yes. And checklists.

Emily Right. And they're hosting a webinar on March twenty fifth specifically about modernizing defenses for instant payment compliance.

Jeff It's worth noting that the expansion to explicit monitoring of ACH credits is a massive operational shift.

Emily Why is.

Jeff That? Well, historically, the banking focus was primarily on unauthorized debits. Someone illegally pulling money out of your account.

Emily Right, like a hacker.

Jeff Exactly. But with the rise of authorised push payment fraud, where a scammer tricks you into willingly sending them money via credit transfer, the regulatory gaze has shifted.

Emily You have to monitor the money you are pushing out, not just the money being pulled. Exactly. And it's not just traditional ACH fiat payments. We have to talk about crypto or crypto. Alex Niu you authored a piece in this research specifically on stablecoins, and it paints a pretty intimidating picture of where financial crime is heading.

Jeff It does, because stablecoins are creating entirely new laundering pathways.

Speaker 3 Oh, so.

Jeff Traditional fiat risk controls were built for banking hours for correspondent banks, for a system with built in friction.

Emily Right. Things take days to clear. Exactly. Crypto moves instantly. Cross-border twenty four over seven with a high degree of pseudonymity. When you apply traditional AML rules to stablecoin flows, you are basically trying to catch a bullet with a butterfly net.

Jeff A butterfly net. That's a great way to put it.

Emily The speed and the on chain off chain hops require an entirely different monitoring framework, which ties right back into why sub one hundred millisecond AI processing is becoming the baseline.

Jeff It's no coincidence, then, that we are seeing a massive mobilization this spring across the industry.

Emily Not at all.

Jeff When you have API blind spots, CBD relief requiring flawless internal cameras, OC risk based exams, and stablecoin laundering all hitting at once, the industry has to respond.

Emily They're all converging.

Jeff And you see it right there on the calendar. CBA Live and Fintech Meetup are happening simultaneously from March thirty to April first, then Fraud Fight Club on April fourteenth and fifteenth, which is this really cool, practitioner driven event for sharing real world strategies.

Emily Yes.

Jeff And then the CPPO Symposium on April 23 for payments professionals.

Emily The cross-pollination of ideas at these events is critical right now. Absolutely. You've got experts fanning out across all of them to share intelligence. Yinglian Xie Unpacking executive insights Regan Smith at CBA Live; Jacob Randall, Michael Rini, Pierre Issensee and Fayez Shafi holding it down at Fraud Fight Club; and Michael Lavia catching the CPPO crowd.

Jeff It's a full court press.

Emily The bad actors share their successful tactics on the dark web instantaneously. The good guys need to be collaborating just as effectively.

Jeff The silos between institutions have to come down, just as the internal silos between fraud and AML departments are coming down, we are moving from isolated fortresses to a networked defense.

Emily So what does this all mean? We have covered a massive amount of ground today.

Jeff We really have.

Emily The overarching, inescapable theme of this deep dive is the urgent, critical shift from reactive compliance to proactive, AI driven defense.

Jeff Without a doubt.

Emily Whether we are looking at the CFPB demanding secure API access without compromising behavioral monitoring or finCEN's beneficial ownership relief, demanding flawless ongoing due diligence or the OCC shifting to strictly risk based exams. The common denominator is relentless.

Jeff It all points in one direction.

Emily Institutions must know their data intimately. They must eliminate their internal silos, and they must have the infrastructure to act on complex risk signals faster than the blink of an eye. You are now fully briefed on the critical fault lines of 2026 financial crime defense.

Jeff Ready for whatever comes next.

Emily If you are heading into a strategy meeting tomorrow, you are ready to ask the tough structural questions. What is our AI readiness gap? How long does it take us to engineer a new feature? Are we relying on legacy batch processing for real time threats?

Jeff Practical questions?

Emily Or if you're just navigating your own digital banking, hopefully you now have a much deeper appreciation for the incredibly complex, invisible armor that is constantly calculating risk to protect your accounts.

Jeff It truly is a remarkable technological achievement. but stepping back. This raises an important question for us to consider as our financial identities become entirely portable through open banking APIs and as our

primary line of defense becomes AI algorithms, calculating complex behavioral risk in under one hundred milliseconds. What happens to the fundamental concept of human trust?

Emily That's a deep question.

Jeff In a system where an offensive AI is relentlessly probing defenses and a defensive AI is constantly updating its algorithms to block it. Are we ultimately protecting the actual human being behind the screen, or are we just protecting the entity, human or machine, who most perfectly mimics the statistically correct digital behavior when AI fights? AI at lightspeed. Where exactly does human intuition fit into the future of our money?

Emily Wow. That is exactly the kind of question that keeps us reading, researching, and questioning the systems around us. Thank you so much for joining us on this deep dive into the fast evolving world of 2026 financial defense. Keep learning, keep questioning, and we will catch you on the next deep dive.

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

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

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

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

Emily 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.