EPISODE 5 | Monthly Brief

February 2026 Nacha and Proactive Detection

FEBRUARY 09, 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 We're digging into the latest newsletter and insights from DataVisor. And honestly, the story that comes out of all this, it's a high stakes race.

Emily It really is.

Jeff You've got threat actors on one side using AI, crypto mixers, you know, the works. And then on the other side you have regulators who are just they're done asking nicely.

Emily They are they're demanding what they call proactive detection.

Jeff And that word proactive, that feels like the key to this whole thing.

Emily Oh, absolutely. That one word is doing a lot of heavy lifting. It's basically the end of an era where you could just report fraud after the fact and and write it off.

Jeff Like the cost of doing business.

Emily Exactly. The new expectation is that you catch it before the money is gone.

Jeff So that's our mission today we are going to unpack how the rules of money are changing right now, with a huge deadline just a few weeks away. We'll get into why speed is the new compliance currency and how tech like unsupervised machine learning is actually saving companies millions.

Emily It's this wild convergence of of policy and some pretty hardcore engineering.

Jeff So let's start with the calendar. March 20, 2026. If you're in US banking, that date should be circled in red.

Emily That's phase one of the new Nacha rules. And yeah, we get rule updates all the time, but this one feels different.

Jeff How so?

Emily It's the mandate itself. It applies to any high volume institution, and it requires, quote, risk based processes. But the real change is the target. They're explicitly going after what they call false pretenses.

Jeff This is a really crucial distinction because for years fraud systems were built to stop hackers, right. Account takeovers. Stolen passwords.

Emily Unauthorized access. Correct. False pretenses is a totally different beast.

Jeff This is where the customer themselves is tricked into sending the money.

Emily Exactly. It's authorized. Push payment fraud or app. So the customer logs in. They pass the biometrics, they click send. They're doing it all themselves. But it's because they're being manipulated.

Jeff The classic romance scam or a fake investment.

Emily Or the grandparent in jail call for a legacy system. That's a nightmare. The transaction looks completely legitimate. The device is right, the IP is familiar, but the intent is fraudulent.

Jeff And this is where the liability starts to shift, right?

Emily Nacha is saying the receiving banks, the rfis, can't just claim ignorance anymore because the login was good. They are now on the hook for detecting that scam.

Jeff So if all the technical signals are clean, what are you even looking for? The notes break this down into three pillars. First one is monitoring inbound credits.

Emily This flips the whole model on its head. For decades, banks have looked at money leaving. The question was always, is my customer being drained? Sure. Now they have to monitor money coming in. They have to watch for accounts that are being used as money mules.

Jeff So you're looking for an account that, say, usually gets one paycheck a month.

Emily And suddenly it's getting ten small transfers from ten different banks in an hour. That's a meal signal. The new rule says you have to be able to flag that inbound traffic to choke off the fraud network.

Jeff Got it. Okay. Pillar two standardized descriptors. This sounds bureaucratic.

Emily does? Haha. It sounds like paperwork, but it's actually an infrastructure play. It's a data quality mandate.

Jeff What do you.

Emily Mean? The rule is forcing specific tags like payroll or purchase into the transaction data. Unstructured data is the enemy of automation. You know, if every transaction is labeled differently, your AI models just see noise.

Jeff So by forcing standard tags, you're cleaning up the data so the algorithms can actually work in real time.

Emily And that brings us to the third pillar, which feels like a legal bear trap. The standard shift.

Jeff This is the one that has the lawyers worried about.

Emily Oh yeah, the standard of liability is moving away from the old, vague, commercially reasonable language.

Jeff Which gives you a lot of gray area in court.

Emily A ton. It's a shield. But the new standard requires documented, annually reviewed procedures. That creates an audit trail. If you miss a huge fraud ring, the regulator can come in and say, show me your procedure from last year's review.

Jeff if you can't prove you updated your defenses against the latest threats.

Emily You're negligent.

Jeff It kills the set it and forget it model of fraud prevention.

Emily You have to prove you're watching the watchers. It's a continuous cycle.

Jeff Okay, so that's the US. Let's widen the lens a bit. The source material suggests Europe is even further ahead on this. The phrase that kept popping up was speed is compliance.

Emily is. Europe is almost always a leading indicator for US regulation. And right now they're penalizing the latency of detection. It's not enough to eventually file a suspicious activity report.

Jeff So filing it three weeks later is now a failure in itself.

Emily It's becoming a regulatory liability. Yes. And this connects to a really fascinating point in the notes about AML fines. You'd think the biggest fines come from, you know, just missing the money laundering. Your AI wasn't smart enough.

Jeff That's not it.

Emily It's not what the data shows. The number one cause of fines is data hygiene.

Jeff The silo problem.

Emily The classic silo problem. The credit card division is on one system checking is on, another mortgage is on a third. The AI model might be brilliant, but if it can't see the transaction from the other department for twenty four hours because of a batch process, it fails.

Jeff Regulators are basically taxing technical debt.

Emily are. And this becomes critical when you look at new powers like instant asset freezing. Authorities can now demand assets be frozen before a conviction.

Jeff Ooh, that is an aggressive power.

Emily Incredibly. And to do that without getting sued by your own customer. You need absolute confidence in your data. You have to verify everything in near real time. If you have to wait for a human to pull records from three systems, the money's gone.

Jeff It's like regulators are demanding that banks operate with the speed of a tech company. Which brings us to crypto.

Emily And specifically stablecoins. Yeah, we've got some notes here from a webinar that really dug into this.

Jeff Stablecoins are such a paradox, aren't they? The name sounds safe, but the source calls them a double edged sword for compliance teams.

Emily Well, you can see the business appeal. High transaction volume. You start processing stablecoins. Your metrics shoot through the roof. It looks like incredible growth.

Jeff The risk doesn't scale linearly.

Emily It's exponential exactly because of what they call the wash and layer capability. You can mine stablecoins with mixers. It's almost the perfect vehicle for breaking that chain of custody. A mixer just tumbles crypto from thousands of sources and spits it back out.

Jeff it's all decentralized. So it's not like you can just call up another bank in the network, right?

Emily That's the challenge. But the counterargument is that the blockchain itself. It's a public, transparent ledger. So a really sophisticated team can actually see more than with a traditional swift transfer.

Jeff But only if you have the tools to actually read the chain.

Emily That's the catch. If you're just treating a stablecoin deposit like cash, you're completely blind to its history. And if that coin just came out of a known mixer, you need to be able to flag it instantly.

Jeff Okay, so the pressure is immense. The complexity is off the charts. Let's pivot to the solution side. How are companies actually fighting back? There's a case study in here about a buy now, pay later provider a BNPL company.

Emily is the perfect stress test, right? The time you have to make a decision is practically zero. You're at checkout. You click buy. That decision has to be made in milliseconds.

Jeff And this provider was getting hammered by new fraud rings. Their old rules based system couldn't keep up, so they switched to unsupervised machine learning. Can you just give us the plain English version of what that means?

Emily Sure. So the standard model is supervised learning. You train it on history, you show it one hundred thousand examples of last year's fraud and say, find more stuff that looks just like this.

Jeff So it's great at catching attacks you already know about.

Emily It's a fantastic pattern matcher for the past. The problem is fraudsters invent new attacks. An unsupervised model works differently. It doesn't need historical labels, it just looks at all the raw data and clusters it. It's designed to say, hmm, I don't know what this group is, but it is behaving statistically differently than ninety nine percent of everyone else.

Jeff So it's spotting the anomaly based on pure behavior. It's like seeing someone walking backward in a crowd. You don't need a rule against walking backward to know that it's weird.

Emily a perfect analogy. And for this BNPL provider, that capability was worth thirty six million dollars in prevented fraud.

Jeff That is a huge number. But the metric that really jumped out at me was the seventy four percent recall rate against emerging rings. What exactly is a recall rate?

Emily Recall is basically the model's ability to find all the bad stuff. So a seventy four percent recall rate against emerging rings means they caught roughly three out of every four attacks from brand new fraud rings the system had never, ever seen before.

Jeff Wow.

Emily is the power of this approach. Catching the unknown unknowns.

Jeff And they did this while reducing false positives by forty one percent. That's usually the trade off, isn't it?

Emily It is. Normally you tighten security. You end up blocking more real customers here because the model is looking at subtle behaviors, not just blunt rules. It got much better at telling the difference between a weird but good customer and an actual fraudster.

Jeff Which led to a five x improvement in review efficiency for their team. And that brings us to the human element. You still need an analyst in the loop.

Emily do, but their job is changing. The notes describe an analyst's day as hunting for a needle in a haystack of widgets. You know, it's just a recipe for burnout.

Jeff And the tool to fix this is something called an interactive investigation checklist. The word checklist sounds a little basic haha.

Emily It does, but this thing is dynamic. It's adaptive. If the AI flags a transaction for, say, a crypto velocity alert, the checklist automatically generates the specific steps for investigating crypto velocity. If it's a mismatched IP, the steps completely change.

Jeff It guides the analysts.

Emily Exactly, and it has zero hunt navigation. So if a step says check device fingerprint, you click it and it takes you right to that data. No more toggling between five different browser windows.

Jeff The feature that seems almost like science fiction, though, is the auto generated summaries.

Emily This is where they use GenAI to actually write the investigation report. After the analyst finishes the checklist, the system synthesizes all the findings into a perfect standardized narrative.

Jeff Which is huge for regulators. They want to see that same logic apply at every single time.

Emily creates consistency, and it frees up the analysts to focus on the hard decisions, not the typing. This all ties back to an article in the source material from Yinglian Jie. She argues that fraud teams have to stop being the Department of No.

Jeff And become a growth driver instead.

Emily Right. If you centralize your tools and monitoring across fraud, cyber and compliance, you're not just stopping bad guys, you're approving more good customers faster. You're reducing friction.

Jeff But there's a huge disconnect between that vision and what's actually happening. Let's talk about this readiness gap.

Emily is the bucket of cold water. There's a survey of AML and fraud leaders. And the numbers are well they're concerning. Seventy four percent of leaders say AI enabled fraud is their number one threat.

Jeff So everybody sees the tsunami coming, but.

Emily They haven't built the seawall. Sixty seven percent, two thirds of the industry admit they lack the data infrastructure to stop it.

Jeff That's what they call agility debt, right?

Emily It's the interest you pay for years of fragmented legacy systems. You just cannot fight AI speed fraud with batch processing mainframes and then regulators add another wrinkle.

Jeff Explainable AI the black box problem.

Emily Yep, we were just praising these complex unsupervised models. But the downside is they can be opaque. A regulator isn't going to accept the computer said so as a reason to freeze a person's life savings.

Jeff You have to show your work.

Emily You have to show your work. It has to be transparent, auditable and defensible. So you need a model that's complex enough to catch the bad guys, but transparent enough to explain itself to a human.

Jeff all of this is happening while the economy is shaky, which always pushes fraud rates up.

Emily Desperation breeds innovation and fraud, so your system has to be flexible. The fraud patterns of twenty twenty four are not the fraud patterns of twenty twenty six.

Jeff So to wrap this all up, we've got a march twenty deadline from Nacha that creates strict liability for scams. We have Europe demanding real time detection. We have crypto creating all sorts of new challenges.

Emily And we have a massive readiness gap where two thirds of the industry admits they aren't equipped to handle the threat that they themselves ranked as number one.

Jeff It seems like the only path forward is to close that agility debt, clean up the data, deploy the new tech.

Emily It is.

Jeff I want to leave you with one final thought. Going back to that auto generated summary feature. Think about it. We have AI detecting the fraud. We have AI guiding the investigation, and we have AI writing the final report.

Emily The machine is handling detection process and documentation.

Jeff Yeah. No. What's the job of a human compliance officer in five years? Are we heading to a world where humans just manage the exceptions? Just audit the algorithms.

Emily think the role gets elevated. You start being a data gatherer and you start becoming a risk strategist. You're the one designing the parameters the AI works within. But the days of manually reviewing every single alert, those are over. The volume is just too high.

Jeff So we move from doing compliance to designing compliance.

Emily That's the shift.

Jeff you want to dig into the details on the Nacha rules, or see the full numbers from that BNPL case study, we'll have the source links in the show notes.

Emily Yeah, definitely check out that false pretenses rule. March twenty is coming up fast.

Jeff It is. Thanks for listening to this deep dive. Keep your data clean and your detectors running.

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's 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.