EPISODE 7 | Analysis

NACHA 2026 Rule Changes Explained

FEBRUARY 23, 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 Check your calendars. Like, seriously, take a second right now and look at the date. If you work in finance, specifically in payments or compliance, today is the one month warning.

Jeff It really is the final countdown.

Emily Because exactly one month from today, on March 20, 2026, the underlying plumbing of the whole US financial system undergoes what might be its biggest renovation in decades.

Jeff And if banks aren't ready, the consequences are going to get very real, very fast.

Emily It sounds super dramatic when we say it like that, but you aren't wrong. We're talking about the 2026 Nacha Operating Rules.

Jeff Which I know sounds incredibly dry.

Emily It sounds like a PDF you just delete without reading. Operating rules like instructions for a microwave or something.

Jeff It usually is. But this time is different.

Emily That's exactly why we're doing this deep dive. Today. We've been pulling apart this comprehensive guide published by DataVisor, along with the official updates from Nacha's own headquarters. Right. We're looking at why the people running the ACH network, this massive system moving trillions of dollars, are suddenly telling banks to stop acting like mailboxes and start acting like bodyguards.

Jeff It's a perfect analogy for fifty years. The bank's main job was just to move money from point A to point B. Right now, they actually have to decide if moving that money is a terrible mistake.

Emily So our mission for this deep dive is pretty simple. We need to figure out what actually happens on March 20th. We need to unpack this concept of "credit push fraud" that everyone in the industry is whispering about. And maybe most importantly, we have to ask ourselves, are we really ready for our banks to start acting like our parents?

Jeff It's a really messy question, but we definitely have to answer it.

Emily Let's start with the crime itself then, because when I hear the word fraud, I have a very specific image in my head.

Jeff The guy in the hoodie.

Emily Yeah, exactly. The hacker in a dark room typing furiously. They steal my password, they log in at three a m, and they just drain my savings account while I'm asleep. I mean, that's fraud, right?

Jeff It is fraud. Absolutely. And the industry, we call that unauthorized fraud. It's a literal break in.

Emily Someone picked the lock, right?

Jeff Someone picked the lock. And for the last thirty years or so, the entire banking security apparatus was built to stop exactly that.

Emily Firewalls, two factor authentication, device fingerprinting.

Jeff All of it. It was castle defense. Just keep the bad guys out. Keep the gate locked.

Emily But looking through this DataVisor Guide, it seems like the castle walls actually held up fine. But the bad guys just completely changed their tactics.

Jeff Yep. They realized the walls were just too high. So instead of trying to break in, they just ask you to lower the drawbridge for them.

Emily And this brings us to the "credit push" concept. Let's make sure we really nail this definition because it's the root of everything that changes next month.

Jeff Think about the difference between a pull and a push. Okay, a debit pull is like your gym membership taking money out of your account every month. You authorized it once and they pull the funds. Right. A credit push is like a wire transfer or a Venmo payment or Zelle. You are actively sending the money out.

Emily So I'm the one initiating it.

Jeff Exactly. And these 2026 rules are a tectonic shift because they specifically address scenarios where that push transaction is technically authorized.

Emily Authorized by me?

Jeff Yes. You logged in, you passed the face ID check, you typed in the account number yourself, and you hit send because.

Emily I thought I was paying a legitimate vendor. Or maybe investing in this guaranteed crypto return.

Jeff Or helping a romantic partner who is magically stuck at customs overseas.

Emily All the classic scams. So business email compromise. BEC is a massive driver here.

Jeff Huge driver. That's the scenario where a CFO gets an email that looks exactly like it's from the CEO saying, why are fifty thousand dollars to this new vendor immediately?

Emily And they just do it.

Jeff They do it. Vendor impersonation, payroll diversion, the Nacha updates list all of these explicitly.

Emily Wow.

Jeff The bank system sees you logging in and says, great, this is the legitimate user. It processes the payment. But in reality, you've been socially engineered.

Emily That phrase socially engineered always gives me the creeps. It implies my brain was hacked, not my computer.

Jeff But that is exactly what happened. The fraudster hacked your trust, not your firewall.

Emily So before these new rules, if I got scammed like that, could the bank just shrug and say, hey, you clicked the button? It's not our problem.

Jeff It's historically. Yes, absolutely. That was the standard offense. The customer authorized it.

Emily Wow.

Jeff The ACH network rules were heavily focused on unauthorized debits. If you pushed the money out yourself, that was on you. You made the mistake.

Emily But this new framework totally flips that table.

Jeff It does. It basically says just because the customer authorized it doesn't mean you can ignore the fact that the transaction looks incredibly suspicious.

Emily That is a massive pivot. It feels like the bank is moving from being a security guard to being like a chaperone.

Jeff I'd call it being an active risk manager. And there's a really important nuance here that DataVisor highlights. The industry calls this fraud induced by false pretenses.

Emily Meaning I was lied to.

Jeff Correct. But here's the kicker Nacha didn't actually create a new legal category for false pretenses. They didn't rewrite US law.

Emily What do they do then?

Jeff They just expanded the definition of suspicious activity. They're telling banks you can't just check the password anymore. You have to check the context. You have to look at the behavior.

Emily Okay, let me play devil's advocate for a second. If I want to send all my money to a prince in Nigeria because I genuinely believe him, does the bank actually have the right to stop me? I mean, it's my money.

Jeff That is the exact tension at the heart of this, and we'll get to the friction it causes later because customers do get furious when you save them from themselves, but from not just perspective. The answer is now yes. If the pattern matches a known fraud typology, like a mule account, the bank has a duty to intervene.

Emily You just mentioned mule accounts, and I think this leads us to what is probably the single biggest operational change in all these documents. We need to talk about the RDFI.

Jeff The receiving depository financial institution. Right.

Emily The bank where the money actually lands.

Jeff This is the real aha moment of the 2026 rules.

Emily Break it down for me. Why is the receiving bank suddenly in the hot seat? Usually if I'm sending money to a scammer, my bank, the sending bank is the one worrying about losing the cash.

Jeff True, the originating bank, the ODFI has always had liability. But think about the actual mechanics of a scam. Okay, if you were being tricked, your behavior might actually look totally normal to your bank. You send money to contractors. You send money to friends.

Emily So my bank doesn't see a red flag because I send wires all the time.

Jeff Right. But the scammer, the account receiving the money. That account looks insane.

Emily Insane? How? Paint the picture for us.

Jeff Imagine a brand new account. It was opened three days ago online. Suddenly, in a span of four hours, it receives fifty separate transfer payments from fifty different people all across the country.

Emily That's a money mule.

Jeff Exactly. Criminals need a way to get money out of the US banking system. They recruit these intermediaries, mules to receive the stolen funds and then immediately wire them offshore or buy crypto. Got it. And the receiving bank is the only one who can see that massive accumulation of funds.

Emily So under the old rules, the receiving bank was just a mailbox. Does the account number match? Yes. Cool. Post the money.

Jeff They were completely passive. They were just the net. Now Nacha says they have to be the goalie.

Emily The DataVisor Guide uses this phrase "lifecycle responsibility," which sounds like corporate speak, but what does it actually mean for a bank manager on the ground?

Jeff It means you own the risk from the moment the account is opened until the day it closes. Okay, let's say you have an old savings account you haven't touched in five years. It's totally dormant. Suddenly it wakes up and receives a fifty thousand dollars payroll deposit from a company you've never worked for.

Emily That's a blazing red flag.

Jeff It is. And under the 2026 rules, the RDFI is required to have risk based fraud monitoring to catch exactly that scenario.

Emily They have to ask if the inbound payment makes sense for that specific customer's history.

Jeff Exactly.

Emily This sounds incredibly expensive for the banks.

Jeff Oh it is, and it's difficult. Monitoring outbound money is somewhat easier because you know, your customer monitoring inbound money. You're judging transactions coming from complete strangers.

Emily But if they succeed, if they shut down the mule accounts.

Jeff Then the whole scam falls apart. If criminals can't receive the money, there's no point in stealing it. You choke off their liquidity.

Emily Okay, so we know who has to watch the receiver. But how? How does a computer know that my payment to Generic Construction LLC is actually a scam without calling me and asking.

Jeff It all comes down to data hygiene, and this is where the new rules get very specific about the toolkit banks have to use. You simply can't spot a pattern if your data is messy.

Emily Garbage in, garbage out.

Jeff Precisely. One of the specific mandates involves the company entry description field. It's that little text blurb you see on your bank statement, right?

Emily The memo line.

Jeff Basically, Nacha is now mandating the strict usage of specific labels like PAYROLL and PURCHASE weight.

Emily Strictly PAYROLL, like all caps spelled exactly like that.

Jeff Yes. If a payment is for wages or salary, it absolutely must use the standard payroll descriptor.

Emily Why does that matter so much? It's just a label.

Jeff Because it allows for automated anomaly detection. Let's go back to your mule account example. If I have an account categorized as personal checking and suddenly I receive five different incoming payments labeled PAYROLL from five different companies in a single week.

Emily Then you either have five full time jobs, which.

Jeff Is pretty unlikely.

Emily Or you are were acting as a money mule collecting payroll diversions from hacked employee accounts.

Jeff Exactly. By standardizing the label, the computer can instantly flag that equation. Personal account plus multiple payroll origins equals high risk.

Emily That makes a ton of sense. Before, if the label was just X affair or fun as s or m l s, the computer couldn't actually tell it was a salary payment.

Jeff Right. And PURCHASE is the other big one. This applies to e-commerce debits.

Emily So if an account that usually only receives Social Security benefits suddenly gets hit with a purchase debit for high end electronics.

Jeff The algorithm wakes up.

Emily But what's the catch? Because there's always a catch with these legacy systems.

Jeff The problem is integration. The DataVisor Guide highlights this as a major hurdle. Banks have their data in silos. The team that handles wire transfers might not even talk to the team that handles ACH.

Emily And neither of them talks to the branch that opened the account five years ago.

Jeff Exactly. To comply with this mandate, banks need a holistic view. They need to connect the dots in real time. The ACH system needs to query the account history database instantly.

Emily Real time is a very scary word in banking. It usually means expensive and highly prone to breaking.

Jeff It is. But it's necessary now because we live in a world of same day ACH.

Emily Let's talk about that tension because as consumers, we want everything faster. I want to pay my credit card bill today. I want my paycheck available immediately.

Jeff It's the eternal struggle, the need for speed versus the need for safety, right?

Emily If the money is moving in two hours, you don't have a human analyst sitting there sipping coffee, leisurely looking at spreadsheets to spot a scam.

Jeff It's impossible. Yeah, manual review is completely dead in this new world. The DataVisor Guide is very clear on this. Compliance requires automated risk based logic. The machine has to decide and it has to decide in milliseconds.

Emily And that scares me a little, because what happens when the machine is wrong?

Jeff That brings us to the customer friction problem, right?

Emily Imagine I'm trying to send money to my contractor for a legitimate kitchen renovation. It's a lot of money. It's a new payee. So the AI looks at and says, nope, looks like a scam.

Jeff And the payment gets blocked. So you get angry, you call the bank, you wait on hold and you yell at a representative. You say, "It's my money, let me send it."

Emily I would be furious. I mean, my kitchen is half finished.

Jeff This is the exact tightrope these banks are walking starting next month. If they stop too many legitimate payments, customers leave because the bank is perceived as broken or too difficult to use.

Emily But if they let too much fraud through.

Jeff They violate the Nacha rules and get hit with fines.

Emily Speaking of, starting next month, let's clarify this deadline. We said March 20, 2026 is that for every single bank or just the big guys?

Jeff Nacha is smart. They did a phased rollout for this. Phase one, which hits on March twentieth, applies strictly to large volume institutions.

Emily What's the cutoff for large volume?

Jeff If you originated more than 6 million entries or received more than 10 million entries in 2023 ? Okay, Basically, if you are a big bank or a major credit union, your deadline is exactly one month away.

Emily And for the smaller community banks, the local credit unions down the state.

Jeff They fall into phase two, June 19, 2026 .

Emily So they have a few more months to panic.

Jeff A few more months to get their house in order. Yes, but the key thing to remember is there is no grace period. None at all. None. Nacha expects compliance on day one, and this also applies to third party senders, the fintechs. Yes, if you are a payroll processor or some shiny new Neobank app that rides on the ACH rails, you are on the hook just as much as the old school legacy banks.

Emily So let me play the cynic here. What if a bank just doesn't do it? What if they look at the cost of upgrading their systems and say, this is too expensive, we're just going to keep doing what we've always done? Is Nacha the police? Can they arrest a bank manager?

Jeff Nacha is definitely not the police. They aren't a government regulator like the Federal Reserve or the CFPB. They are a private rulemaking body.

Emily So they have no teeth.

Jeff Oh, they have teeth, but they aren't legal teeth. They are contractual teeth.

Emily Explain how that works.

Jeff Participation in the ACH network is technically voluntary. You agree to follow the rules so you can play the game. If you don't follow the rules, Nacha can audit you, they can investigate.

Emily And then what?

Jeff They can levy class three rules violations which carry some very significant financial penalties.

Emily Okay, fines are bad, but big banks pay fines all the time. It's practically a line item in their annual budget.

Jeff True, but the nuclear option is restricting access to the network.

Emily Oh, wow.

Jeff Yeah. In extreme cases, if a participant is threatening the actual integrity of the network, say, by letting a massive amount of fraud flow through unchecked play, they can be restricted.

Emily Imagine a bank that literally cannot process direct deposits or pay bills electronically.

Jeff That's a death sentence. It's an extinction event for a modern bank. So while Nacha isn't the police, they are the landlord and they can evict you.

Emily That really puts it in perspective. This isn't a friendly suggestion from an industry group. It's a requirement for survival.

Jeff And it really aligns with the global trend we are seeing. If we look at the big picture, the UK has been doing this with their confirmation of payee system. Other countries are enforcing similar liability shifts.

Emily So the US is just playing catch up.

Jeff Exactly. We are finally moving from a reactive model where we just try to clean up the mess after the money is already gone, to a proactive model.

Emily Where active sounds great on paper. Identifying the risk before the money moves. But I want to circle back to something we touched on earlier about the false pretenses.

Jeff Sure.

Emily Go ahead. We are building a system where the bank actively monitors for intent. They are trying to figure out if you, the customer, are being tricked, right?

Jeff That's the ultimate goal of the behavioral analytics.

Emily So here's the thought I want to leave everyone with as we wrap up this deep dive. And it's a bit uncomfortable.

Jeff Let's hear it.

Emily If you woke up tomorrow and willingly sent money to a scammer because you truly, deeply believed in the lie they told you, would you actually want your bank to stop you.

Jeff I think most people would immediately say yes. Protect me. Protect my life savings.

Emily In theory, sure. But imagine being in that moment. You are completely convinced. You think you are in love, or you think you've just found the real estate investment of a lifetime. You are excited to send this wire and the bank just says no. They treat you like a child who can't be trusted with their own allowance.

Jeff It is incredibly paternalistic.

Emily It is. Are we ready for a banking relationship that feels less like a service provider and more like a parent child dynamic? Because looking at these 2026 rules, that is effectively what we are building a safety net that in the heat of the moment might feel a lot like a cage.

Jeff It's true security always comes at the cost of liberty. We are just trying to find where the new balance point is in a digital world.

Emily Indeed we are. And for the compliance officers listening to this, staring at that March twentieth date on the calendar right now. Good luck. You're really going to need it.

Jeff Get those algorithms ready.

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.