COMPLIANCE GUIDE

The NACHA 2026 Fraud Rules and Deepfakes: What Every Financial Institution Must Know Before June 19

By Brian Koyundi, Founder — Deeptrack Inc. *Published April 2026* 5 min read

KEY TAKEAWAYS

NACHA's 2026 operating rule changes introduce the first formal mandate for proactive, risk-based ACH fraud monitoring across the entire US payments network. Phase 1 (March 20, 2026) is already in effect for high-volume institutions. Phase 2 (June 19, 2026) extends obligations to every non-consumer originator regardless of volume. Synthetic identity fraud and deepfake-enabled account opening are the highest-risk attack vectors under the new rules — and most institutions are not yet equipped to detect them. This guide explains what the rules require, where deepfakes enter the ACH chain, and what compliance looks like in practice.

The ACH network processes more than 31 billion transactions annually, moving approximately $80 trillion through the US economy. For most of its history, fraud monitoring on that network was largely reactive and narrowly scoped. Financial institutions monitored certain debit transactions. Everyone else largely watched and waited.

That era is over.

NACHA's 2026 operating rule changes the most significant update to ACH fraud obligations in a generation establish for the first time a formal, network-wide requirement for proactive, risk-based fraud monitoring. And the fraud vectors driving those changes are not the familiar ones. They are synthetic identities. Deepfake credentials. AI-generated voices authorising payroll transfers. Fabricated documents that no human eye can distinguish from the real thing.

> ***The rule changes are not primarily about catching the fraudsters who already got in. They are about closing the door on AI-generated identities that should never have been admitted in the first place.***

This guide walks through the new NACHA requirements, explains where deepfakes and synthetic identities fit into the ACH attack surface, and outlines what compliance controls look like in practice. A 12-item compliance checklist is included at the end.

What the NACHA 2026 rules actually require

The new rules target a specific category of fraud that NACHA defines as 'entries initiated under false pretenses' transactions that are technically authorised by the legitimate account holder, but only because that person was deceived. Business email compromise, vendor impersonation, payroll fraud, and deepfake-enabled CEO fraud all fall under this definition.

The core obligation is straightforward: institutions must establish 'risk-based processes and procedures reasonably intended to identify ACH entries initiated due to fraud.' What that means in practice is significantly less straightforward, because NACHA deliberately did not prescribe

specific technical controls. The rule is principles-based, which gives institutions flexibility but also creates compliance ambiguity.

THE TWO-PHASE ROLLOUT

Phase 1 (effective March 20, 2026): Applies to all ODFIs and to Originators, Third-Party Senders, and Third-Party Service Providers whose 2023 ACH origination or transmission volume exceeded 6 million entries. If your institution was in scope for Phase 1, you are already required to comply. Phase 2 (effective June 19, 2026): Eliminates the volume threshold entirely. Every non-consumer Originator, Third-Party Service Provider, and Third-Party Sender — regardless of how many ACH entries they originate — must comply. June 19 is the date that makes this universal.

The monitoring obligation extends to both sides of the transaction. ODFIs - the banks sending ACH credits must monitor outgoing transactions for signs of fraud. RDFIs - the banks receiving those credits must monitor inbound transactions and are now empowered to initiate returns of suspicious funds without waiting for the ODFI to flag the transaction. This is a material shift from the previous model, where RDFIs were largely passive processors.

Additionally, institutions must review their monitoring processes annually and demonstrate that those processes evolve with the fraud landscape. A static rule set implemented in 2024 and never updated will not satisfy the 2026 requirements when examined.

Where deepfakes and synthetic identities enter the ACH chain

The NACHA rules do not mention deepfakes by name. They do not need to. The attack patterns that the rules are designed to prevent impersonation-based fraud, false-pretence account openings, synthetic identity schemes are exactly the scenarios where deepfakes and AI-generated media are now the primary tools.

There are three primary entry points where synthetic media attacks intersect with ACH fraud risk.

Account opening and KYC bypass

The fastest-growing attack vector in 2025 was not phishing or credential theft. It was synthetic identity fraud at account opening. US lenders faced $3.3 billion in exposure from synthetic identities in just the first half of 2025. Synthetic identity document fraud surged 311% in North America in Q1 2025 alone.

The attack is structurally simple: a fraudster creates a plausible identity by combining a real Social Security number (often from a child or recent immigrant with no credit history) with fabricated name, address, and contact information. They then use AI-generated facial imagery to pass liveness detection checks during digital onboarding. The account is opened, passes KYC, and begins accumulating ACH credit history. Months later sometimes years later the account is weaponised for fraud before disappearing.

Under the new NACHA rules, an institution that cannot demonstrate that its KYC controls would have detected this attack pattern is exposed to examination risk.

Payroll and vendor impersonation

The second attack vector is executive impersonation used to redirect ACH payroll or vendor payments. This is the 'false pretenses' scenario NACHA is most directly targeting. A finance employee receives what appears to be a video call or voice message from a senior executive

authorising an urgent payroll file update or vendor payment change. The instruction is followed. The funds leave via ACH. The executive never made the call.

Deepfake-enabled vishing attacks surged by more than 1,600% in Q1 2025 compared to Q4 2024. The technology required to produce a convincing voice clone costs less than $10 and requires as little as three seconds of audio. The barrier to entry for this attack has collapsed.

> ***A fraudster creates a synthetic identity and opens a checking account. Days later, multiple payroll direct deposits start flowing in but none match the identity of the account holder. Under the new NACHA rules, the RDFI is now responsible for catching this.***

Under the new NACHA rules, institutions must be able to identify these patterns. An RDFI receiving payroll ACH credits into an account that exhibits anomalous recipient patterns or mismatched identity signals must now have controls capable of flagging and potentially returning those entries.

AI-generated document fraud

The third vector is fabricated documentation used to support ACH transactions fraudulent pay stubs, bank statements, invoices, and tax records generated entirely by AI. These documents are not altered versions of real documents. They are created from scratch with realistic formatting, logos, and signatures designed specifically to bypass document verification checks.

Advances in generative AI have made this type of fraud accessible to non-technical actors. The documents that previously required specialised forgery skills can now be produced in minutes. Institutions that rely on document scanning and OCR as their primary fraud control are operating with a fundamentally broken assumption: that documents presented for verification have a real physical or digital origin.

What compliance looks like in practice

NACHA's principles-based approach means that no single control is prescribed. But regulators examining compliance will look for three things: that an institution understood its fraud risk, that it implemented controls proportionate to that risk, and that those controls can actually detect the fraud patterns in scope. Here is what that translates to in operational terms.

Liveness detection that can withstand injection attacks

Traditional liveness detection asks users to perform actions blink, turn their head, smile to confirm they are physically present. This works against masks and photographs. It does not work against injection attacks, where AI-generated video is fed directly into the biometric verification system at the software level, bypassing the camera entirely.

The control that satisfies NACHA's requirements is multi-signal liveness detection: systems that combine behavioural signals (eye movement patterns, micro-expressions, breathing artefacts) with hardware-level signals (device attestation, camera integrity checks) and model-level deepfake detection. Any single-signal liveness check is now a compliance gap.

Continuous monitoring, not checkpoint verification

The NACHA rules explicitly require monitoring across the full transaction lifecycle, not just at account opening. A one-and-done KYC check is insufficient. Institutions need monitoring that

covers account opening, transaction initiation, and ongoing behavioural patterns including ACH credit receipt patterns that do not match the established profile of the account holder.

Gartner's 2026 prediction is blunt: 30% of enterprises will no longer consider standalone identity verification solutions reliable in isolation. Layered, continuous monitoring is the direction of travel, and the NACHA rules formalise that expectation for the ACH network.

Audit trails for regulatory examination

Principles-based rules are enforced through examination. When a NACHA examiner reviews your institution's fraud monitoring program, they will ask for documentation: what signals did your systems evaluate, what decisions were made, and on what basis. Institutions that cannot produce a clear forensic record of their fraud detection logic including confidence scores, detection model outputs, and decision rationale will struggle to demonstrate compliance.

This is where the distinction between detection and documentation becomes operationally significant. Detecting a synthetic identity is necessary but not sufficient. Being able to explain, with precision, how and why that detection occurred and to reproduce that explanation for an examiner is what compliance actually requires.

The June 19 deadline and what it means for your institution

If your institution originates ACH payments and was not in scope for the March 20 Phase 1 deadline, you have until June 19, 2026. That is approximately eight weeks from the date of this publication.

Eight weeks is enough time to implement meaningful controls if you start now. It is not enough time if you are beginning a procurement process, a vendor evaluation, or an internal approval cycle from scratch. Institutions that have not yet assessed their gap exposure against the new requirements should treat this as urgent.

THE EXAMINATION RISK

Weak controls around ACH credits, payroll files, or vendor payments translate into NACHA exam findings, enforcement actions, and reputational damage that extends beyond any individual penalty. NACHA's 2026 rule changes make this risk explicit: non-compliance with the new false pretences monitoring requirements is now a defined enforcement risk. This is not a speculative future risk. Phase 1 is already in effect.

The institutions most exposed are not necessarily the largest. High-volume institutions have been preparing since Phase 1 was announced. The Phase 2 extension to all originators regardless of volume is specifically designed to close the compliance gap at mid-market fintechs, payroll processors, and ACH-originating non-bank financial institutions entities that have historically operated with minimal fraud monitoring obligations and may have invested accordingly.

Compliance checklist — 12 items

The following checklist maps the core NACHA 2026 compliance obligations to operational controls. It is designed for internal distribution to compliance, fraud, and technology teams. Download the formatted PDF version at deeptrack.io/resources/nacha-2026-checklist.

#	Compliance requirement	Applies to	Deeptrack covers
1	Establish documented risk-based ACH fraud monitoring policies and procedures	ODFIs, all Originators (Phase 2)	
2	Monitor ACH credits and debits — not just consumer WEB debits	ODFIs, RDFIs, Originators	
3	Identify entries initiated under false pretenses (impersonation, vendor fraud, payroll fraud)	ODFIs, Originators	✓ Gotham
4	Implement liveness detection resistant to injection attacks at account opening	ODFIs, KYC teams	✓ Sentinel
5	Deploy synthetic identity detection across digital onboarding flows	All originators	✓ Sentinel
6	Monitor inbound ACH credit patterns for anomalous recipient identity signals	RDFIs	
7	Maintain forensic audit trails of fraud detection decisions with model-level detail	All in-scope entities	✓ Gotham
8	Detect AI-generated documents submitted to support ACH transactions	Originators, fintechs	✓ Foundry
9	Implement multi-signal voice and video verification for executive instruction channels	ODFIs, corporates	✓ Gotham
10	Review and update fraud monitoring processes at least annually	All in-scope entities	
11	Establish rapid-return capability for suspicious ACH credits without ODFI initiation	RDFIs	
12	Document compliance posture for NACHA examination — not just detection but explanation	All in-scope entities	✓ Gotham

What to do next

If your institution has not yet mapped its current fraud controls against the NACHA 2026 requirements, start with items 1, 3, 4, and 7 on the checklist above. These four controls represent the highest examination risk for institutions that have historically relied on document scanning and one-time liveness checks as their primary fraud barrier.

The June 19 deadline is not the finish line. It is the floor. The institutions that will outperform over the next 24 months are those treating this rule change as a signal to build continuous, AI-resistant fraud monitoring infrastructure not a compliance checkbox to be satisfied and forgotten.

Deeptrack's Gotham and Sentinel products were built for exactly this operational context: multi-modal detection with full forensic audit trails, designed to integrate into existing KYC and AML stacks without a platform rebuild. If you want a compliance briefing tailored to your institution's ACH profile, contact us at bryan@deeptrack.io.

About Deeptrack Deeptrack is an AI-powered deepfake detection platform built by Brian Koyundi in Nairobi, Kenya. Its flagship enterprise product, Gotham, provides multi-modal detection (video, audio, image, document) with forensic scoring and audit trails for financial institutions, media organisations, and government agencies. Deeptrack is a member of the C2PA (Coalition for Content Provenance and Authenticity) and integrates with Reality Defender's detection API. Contact: bryan@deeptrack.io · deeptrack.io

Sources: NACHA Operating Rules (2026), Oscilar ACH Fraud Report 2026, BIIA Synthetic Identity Fraud Statistics 2026, Keepnet Deepfake Statistics 2026, PYMNTS NACHA Analysis April 2026, Gartner Identity Verification Predictions 2026, PwC Fraud Trends 2026, Sumsub Identity Fraud Report 2025.

Appendix — Abbreviations and key terms

All abbreviations used in this article are defined below for readers unfamiliar with US payments regulation terminology.

Abbreviation	Full term	Plain-language definition
ACH	Automated Clearing House	The electronic network that processes direct deposits, payroll, bill payments, and bank-to-bank transfers in the United States. When your salary arrives as a direct deposit or you pay a bill by linking your bank account, that transaction moves through the ACH network.
NACHA	National Automated Clearing House Association	The governing body that sets and enforces the operating rules for the US ACH network. NACHA is not a government regulator but its rules carry regulatory weight because all ACH participants must agree to follow them as a condition of network access.
ODFI	Originating Depository Financial Institution	The bank on the sending side of an ACH transaction — the institution that originates the payment into the network on behalf of the company or individual initiating it. If a business runs payroll through ACH, its bank is the ODFI.
RDFI	Receiving Depository Financial Institution	The bank on the receiving end of an ACH transaction — the institution that posts the funds into the recipient's account. Under the 2026 NACHA rules, RDFIs now carry active monitoring obligations and can return suspicious funds without waiting for the ODFI to act.
KYC	Know Your Customer	The identity verification process banks and financial institutions use when onboarding new customers. KYC typically includes document verification, liveness detection, and sanctions screening. It is the primary point of vulnerability for synthetic identity and deepfake attacks.
KYB	Know Your Business	The equivalent of KYC applied to business entities rather than individuals. When a company opens a business bank account or applies for credit, the institution runs KYB checks to verify the business is legitimate and to identify its beneficial owners.
AML	Anti-Money Laundering	The set of laws, regulations, and procedures designed to prevent criminals from disguising illegally obtained funds as legitimate income. Financial institutions are required to have AML programs that monitor transactions for suspicious activity and report it to regulators.
BEC	Business Email Compromise	A fraud scheme where attackers impersonate a company executive, supplier, or colleague via email to trick an employee into authorising a payment or transferring funds. BEC is one of the highest-value fraud categories globally and is increasingly augmented by deepfake audio and video.
GAN	Generative Adversarial Network	The AI architecture that powers most deepfake generation. A GAN pits two neural networks against each other: one that generates synthetic media and one that tries to detect it. They train each other until the fakes become difficult or impossible to distinguish from genuine content.
IDV	Identity Verification	The process of confirming that a person is who they claim to be, typically by checking their identity documents, biometrics, and liveness. IDV is a component of KYC and is the primary attack surface for deepfake injection attacks.

TPS / TPSP	Third-Party Sender / Third-Party Service Provider	Non-bank entities that originate or process ACH transactions on behalf of businesses. Payroll processors, fintech platforms, AP/AR software providers, and payment intermediaries typically fall into this category. Phase 2 of the NACHA 2026 rules brings all TPS and TPSP entities into scope for the first time.
C2PA	Coalition for Content Provenance and Authenticity	An industry standards body developing technical specifications for embedding verifiable provenance metadata into digital media. C2PA standards allow media files to carry a tamper-evident record of their origin, creation tool, and edit history. Deeptrack is a member of C2PA.
Vishing	Voice phishing	A social engineering attack conducted by phone or voice message, often using a cloned or AI-generated voice to impersonate a trusted person. Deepfake-enabled vishing attacks surged 1,600% in Q1 2025 compared to Q4 2024.