Social engineering is now an examination priority

A Netarx briefing for SEC, OCC, FinCEN, and NCUA regulated firms.

On October 23, 2026, the Securities and Exchange Commission's Division of Examinations named synthetic and deepfake voice and video used for social engineering as a fiscal year 2027 examination focus, and routed it into the identity theft prevention program and the customer information safeguards. It is not alone in saying so. FinCEN, the Treasury Department, the OCC, the federal banking agencies, and the National Credit Union Administration have each put the same attack class in writing, and their expectations point the same direction even where the authority behind them differs.

This briefing sets the published language side by side, authority by authority, then lists the questions a regulated firm should be able to answer today.

1. Six regulators, one attack class

Authority	Instrument	What it says about this attack class
SEC, Division of Examinations	Examination Priorities, Fiscal Year 2027 (Oct. 23, 2026)	Examinations will focus on "registrants' assessment and preparation for potential threats from SI-related cyberattacks that may affect their businesses or customers, such as SI-generated phishing messaging and synthetic or deepfake voice and video used for social engineering." Routed into two named programs: the identity theft prevention program under Regulation S-ID, and incident response and customer notification under Regulation S-P.
FinCEN	Alert FIN-2024-Alert004, "Fraud Schemes Involving Deepfake Media Targeting Financial Institutions" (Nov. 13, 2024)	Typologies of deepfake-enabled fraud, red flag indicators for identifying and reporting related suspicious activity, and a reminder of Bank Secrecy Act reporting obligations.
U.S. Treasury	2026 National Money Laundering Risk Assessment (March 2026)	A dedicated section, "Use of AI in Fraud and Scams." It reports voice clones, fake profiles, and video "with believable depictions of public figures or even loved ones," which "accelerate the existing risks of phishing … and social engineering," and cites Bank Secrecy Act data on accounts opened with identities produced by generative AI.
OCC	Bulletin 2026-54, "Super Intelligence: Supervisory Framework" (Nov. 4, 2026)	The OCC's first examiner framework for how banks use SI, including agentic systems. It addresses the institution's own deployment, not an attacker's use of the same tools.
Federal Reserve, OCC, FDIC	Revised interagency model risk management guidance, SR 26-2 / OCC Bulletin 2026-13 (April 17, 2026)	Rescinds SR 11-7 and states that "generative AI and agentic AI models are novel and rapidly evolving" and "are not within the scope of this guidance." The tooling an attacker uses to build a voice clone sits outside that scope by design.
NCUA, and state credit union supervisors	12 CFR Part 717, Appendix J; Letter 26-CU-01, 2026 Supervisory Priorities (Jan. 2026)	A federal credit union must keep a written identity theft prevention program and update its red flags periodically "to reflect changes in risks to members." Fraud prevention stays in the 2026 exam scope, and NCUA's artificial intelligence resource page sends credit unions to FinCEN's deepfake alert for "specific red flag indicators" and identity verification practices.

Federal agencies write "super intelligence (SI)" where earlier documents said "artificial intelligence," under Executive Order 14434.

For banks and credit unions, three separate rules carry one instruction: Regulation S-ID, the banking agencies' Interagency Guidelines, and the NCUA's 12 CFR Part 717 each require re-identifying red flags as the methods of identity theft change. A cloned voice added to a payment instruction is a change in method.

2. The questions a firm should be able to answer

"Completed annual awareness training" is not an answer to any of these.

1. Which written policy covers impersonation of an executive, a vendor, or a family member by voice or video, as distinct from phishing by email?
2. When a payment or account change arrives by voice or video, what independent signal confirms the person?
3. When a live call is in progress and the voice or face looks wrong, what happens before the money moves?
4. How does the identity theft prevention program reflect a stolen credential combined with a synthetic face, as distinct from a stolen credential alone?
5. Under Regulation S-P, who is notified, within what window, and how is a service provider's incident counted?
6. What did the last test measure: false negatives, false positives per user per day, and help desk tickets attributable to verification?

Questions 4 through 6 are the ones with documents behind them. A firm that can produce an updated red flag inventory, an incident response program that names synthetic media, and test results will spend its examination time on other subjects.

3. Why the standard stack does not answer them

- **Email filtering** scores a message and its sender. It receives no audio and no video.
- **Multi-factor authentication** confirms a device or a secret. It authenticates a session. It does not establish who is on the other end of a call.
- **Awareness training** asks a person to detect a synthetic voice in real time, under pressure, with money moving. The Department of Homeland Security report cited by FinCEN is direct on the mechanism: synthetic media "do not need to be particularly advanced or believable to be effective."
- **Third-party review** usually stops at the software the firm deployed. It does not cover the tools an attacker points back at the firm.

4. A 30-day proof plan

Pick one department, 20 to 50 people. We only need 2 hours with your team, and you run it for 30 days. You'll be able to satisfy the examiners and tell the C-suite that you've already installed the first phase of social engineering protection tools to safeguard against the AI maelstrom that has already begun.

Sources

- **SEC Division of Examinations, Examination Priorities, Fiscal Year 2027** (Oct. 23, 2026; announced in Press Release 2026-109): sec.gov/files/2027-exam-priorities.pdf
- **Executive Order 14434, "Inaugurating the Era of Super Intelligence"** (signed Sept. 29, 2026; 91 FR 63129): federalregister.gov/documents/2026/10/02/2026-20321
- **FinCEN Alert FIN-2024-Alert004, "Fraud Schemes Involving Deepfake Media Targeting Financial Institutions"** (Nov. 13, 2024): fincen.gov/system/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf
- **U.S. Treasury, 2026 National Money Laundering Risk Assessment** (March 2026): home.treasury.gov/system/files/246/2026-NMLRA.pdf
- **OCC Bulletin 2026-54, "Super Intelligence: Supervisory Framework"** (Nov. 4, 2026): occ.gov/news-issuances/bulletins/2026/bulletin-2026-54.html
- **OCC Bulletin 2026-13 / Federal Reserve SR 26-2, "Model Risk Management: Revised Guidance"** (April 17, 2026): occ.gov/news-issuances/bulletins/2026/bulletin-2026-13.html
- **Identity Theft Red Flags: Interagency Guidelines** (12 CFR Part 41, Appendix J for banks; 12 CFR Part 717, Appendix J for federal credit unions): ecfr.gov/current/title-12/part-717/subpart-J
- **NCUA Letter 26-CU-01, "NCUA's 2026 Supervisory Priorities"** (Jan. 2026), and the NCUA artificial intelligence resource page: ncua.gov/regulation-supervision/regulatory-compliance-resources/artificial-intelligence-ai