SECURITY BASECAMP LLC | 2026 THREAT INTELLIGENCE SERIES

Detecting Deep Fakes & Preventing Fraud

Practical guidance for compliance leaders and financial services firms navigating
AI-enabled identity fraud and synthetic media attacks.

Security Basecamp
CYBERSECURITY & COMPLIANCE

SEC FINRA NYDFS

⚠ **Deepfake fraud losses in financial services exceeded $200M in 2024 — and AI tools have made high-quality forgeries accessible to non-technical threat actors.**

Deepfake technology — AI-generated audio, video, and synthetic identities — has crossed from science fiction into everyday fraud. Voice cloning tools now require only seconds of audio to replicate a CFO's voice. Video synthesis can fabricate real-time executive calls. For financial services firms, this means traditional identity verification methods — voice recognition, video, email — can no longer be trusted as authoritative proof of identity.

HOW DEEPFAKES ARE BEING USED TO STEAL MONEY

🏦 CEO / CFO WIRE FRAUD

AI-synthesized voice or video of a firm's CFO or CEO directs finance staff to execute urgent wire transfers — often combined with spoofed email and a fabricated business justification. Average loss per incident: $500K+.

📞 VENDOR PAYMENT HIJACKING

Attackers clone a known vendor's voice and call accounts payable to redirect ACH or wire routing to a fraudulent account. A convincing callback to a spoofed number provides false confirmation.

👤 SYNTHETIC IDENTITY FRAUD

AI-assembled identities combine real PII fragments with generated photos and documents to pass KYC/AML onboarding checks, open accounts, and initiate fraudulent withdrawals before detection.

🎥 FAKE EXECUTIVE VIDEO CALLS

Real-time deepfake video of senior executives is used in live video calls to authorize transactions, extract credentials, or manipulate counterparties — making the fraud nearly indistinguishable from a legitimate meeting.

🔑 MFA & HELPDESK BYPASS

Attackers impersonate IT staff or employees using AI voice cloning to trick helpdesks into resetting passwords, disabling MFA, or granting system access — the same attack vector used in the MGM Resorts breach.

✉ EXECUTIVE COMMUNICATION FORGERIES

Fabricated emails, voice memos, and even short video clips attributed to firm leadership are used to pressure staff into bypassing financial controls or disclosing sensitive credentials.

WARNING SIGNS YOUR TEAM SHOULD RECOGNIZE

AUDIO / VOICE INDICATORS

- Flat, slightly robotic cadence or pacing
- Unusual background silence or artificial room tone
- Slight delay between speech and lip movement
- Voice quality inconsistent with known caller
- Caller avoids direct questions or deviates from script

VIDEO CALL INDICATORS

- Blurry or flickering face/hair edges, especially in motion
- Inconsistent lighting or skin tone across the frame
- Eyes or teeth that don't render naturally
- Lip sync slightly mismatched with audio
- Background loop or subtle visual artifacts

BEHAVIORAL RED FLAGS

- Extreme urgency — "must happen today / before close"
- Request to bypass normal approval channels
- New payment account or routing details provided verbally
- Request to keep transaction confidential from others
- Out-of-pattern communication channel (e.g., WhatsApp)

IDENTITY VERIFICATION FAILURES

- ID documents with inconsistent fonts, shadows, or metadata
- Profile photos that fail reverse image search
- PII that matches stolen data breach records
- Liveness check failure in onboarding tools
- Mismatches between stated identity and behavioral patterns

RECOMMENDED CONTROLS

DUAL AUTHORIZATION

All wire transfers above a defined threshold require approval from two separate individuals through independent channels. One instruction alone — regardless of source — is never sufficient.

OUT-OF-BAND VERIFICATION

Any instruction received by voice, email, or video that requests financial action must be verified through a pre-established secondary contact method — not a number provided in the original request.

VENDOR CHANGE CONTROLS

Documented procedures for any change to vendor payment routing, including mandatory callback to a pre-verified number and written confirmation. No verbal-only authorization accepted.

DEEPFAKE AWARENESS TRAINING

Ongoing staff training covering AI voice cloning, video synthesis, and social engineering tactics. Employees must know that voice alone is never sufficient authorization for financial action.

AI DETECTION TOOLING

Deploy platforms capable of detecting synthetic media in email attachments, video calls, and identity documents. Integrate liveness checks into customer onboarding workflows.

INCIDENT RESPONSE READINESS

Maintain a tested incident response plan that specifically addresses deepfake fraud scenarios, including escalation paths, regulatory notification timelines, and forensic preservation steps.

RECOMMENDED SOLUTIONS FOR DETECTION & PREVENTION

Pindrop

VOICE AUTHENTICATION

AI-powered voice fraud detection for contact centers. Identifies deepfake and cloned voice attacks in real time during live calls.

Jumio

IDENTITY VERIFICATION

Biometric identity verification with liveness detection and document authenticity checks — designed to stop synthetic identity fraud at onboarding.

Sensity AI

DEEPFAKE DETECTION

Enterprise deepfake detection platform covering video, audio, and image forgeries. Used by financial institutions and government agencies for threat analysis.

Reality Defender

SYNTHETIC MEDIA DETECTION

Real-time deepfake detection API for video calls, uploaded media, and communications. Integrates with existing security and compliance workflows.

ID.me / Persona

KYC / IDENTITY

Identity proofing platforms with government ID verification, facial biometrics, and synthetic identity fraud detection for regulated onboarding flows.

Microsoft / Nuance

VOICE BIOMETRICS

Enterprise voice biometric authentication with anti-spoofing for contact centers. Part of Microsoft's integrated security suite for financial services.

TABLETOP EXERCISE: WOULD YOUR CONTROLS STOP THIS?

A caller claiming to be your CEO contacts your finance department using a voice that passes recognition. The call is urgent: wire $500,000 to a new account before market close today. Your CEO is unreachable by normal channels. Walk through this scenario with your team — the answer reveals gaps in your current controls before a threat actor does.

Security Basecamp helps firms detect and mitigate cybersecurity threats and vulnerabilities. We help you respond to and recover from cybersecurity incidents while staying SEC, FINRA, and NYDFS compliant. Together, the team has completed hundreds of Cybersecurity Risk Assessments, Penetration Tests, Vendor Risk Assessments, and custom cybersecurity projects exclusively focused on the financial services industry. The team includes highly credentialed cybersecurity experts — CISSPs, Security+, PenTest+, GIAC certified professionals — who share a mission to proactively manage and mitigate risks while strengthening defenses against emerging threats in a complex regulatory environment.

securitybasecamp.com | (949) 330-0899 | info@securitybasecamp.com

Security Basecamp LLC