AFFINITY FRAUD: DEEPFAKES IN THE DIASPORA

Posted on December 9, 2025 by Keghart



Category: Opinions

By **Heidi Boghosian**, New Jersey, Armenian Weekly, 1 December 2025

This article first appeared in The Armenian Weekly and is republished with permission.

The "law student" who contacted me online and later joined a Zoom call seemed credible. He said he'd found my email through the Armenian Bar Association, spoke with a light accent and referenced community life. His posture felt stiff, but I chalked it up to nerves. Only after a series of urgent messages did the truth surface: he wasn't a person at all, but a synthetic construct stitched from fragments of data, voice and likeness — a deepfake engineered to exploit cultural familiarity, name-based trust and ultimately, steal my money.

> *Research on diaspora communities shows a clear pattern: when a message appears to come from "one of our own," skepticism drops.*

Scammers and disinformation actors understand this and increasingly tailor scripts, accents and cultural cues to mimic belonging. Regulators call this affinity fraud, deception designed to blend so seamlessly into community life that it bypasses rational doubt. Armenian networks, like many diasporas, run on trust — in schools, churches, cultural institutions and philanthropic projects. That trust is a strength, but it can turn into a vulnerability when weaponized.

Recent events show how quickly synthetic media can infiltrate public perception. Earlier this year, Armenia's Personal Data Protection Agency warned about an AI-generated video featuring a fabricated message from Prime Minister Nikol Pashinyan promoting a fake investment opportunity promising viewers a monthly income of 1.8 million dram — about $4,500 — complete with patriotic framing: "The future of our people is in your hands," — and an invitation to enroll through a link.

A few months later, the fact-checking outlet CivilNet uncovered a wave of similar scams, including deepfakes of renowned surgeon Bagrat Alekian pitching miracle cures built from repurposed interview footage and distributed anonymously across suspicious foreign-run pages.

They target what binds us, including language, culture and the assumption that when we see one another online, we're seeing something real. Affinity fraud can now strip an unsuspecting person of their savings and identity in a matter of minutes.

These manipulations aren't random — they are engineered to hit emotional pressure points, including national pride, health fear and economic insecurity. In a region accustomed to disinformation warfare, deepfakes mark a new terrain.

Diasporas carry layered loyalties shaped by concern for relatives, reverence for cultural authority and a predisposition to respond to messages from familiar names. That dynamic provides fertile ground for synthetic identities to pose as community leaders, relatives or credentialed experts — asking for donations, personal data or participation in fraudulent schemes. Yet, no mechanism currently exists to measure how widespread these attempts have become.

Family sits at the core of Armenian life, older than borders, older than statehood. Through exile and genocide, it carried language, faith, memory. In the diaspora, it became a quiet guarantee: if someone sounds like us, they must be safe.

Deepfakes weaponize that instinct. A familiar face, a comforting cadence — the signals of belonging — can short-circuit caution.

> *If we mean to protect one another, digital literacy must join language and history as part of our inheritance. Verification isn't cynicism. It's care.*

Tips to avoid deepfake scams targeting Armenians

1. **Slow down before responding — urgency is a red flag.**

If someone claiming to be Armenian pressures you, uses emotional language ("*akhper* jan," "*kuyrik* jan," "urgent help!"), or demands fast action, pause. Scammers rely on cultural familiarity to bypass skepticism.

2. **Verify identity using a second channel.**

Ask to confirm identity through a known mutual connection, community organization or platform you already trust. Example: "Before we continue, can you share who you know at the local Armenian church, school or community group?" Real people won't object. Scammers often vanish.

3. **Use a *challenge question* only a real Armenian would answer — but avoid anything publicly searchable.**

Instead of: "Where are your parents from?" (easy to fake), ask:

- A personal connection ("Who introduced you at last year's program?")
- A shared memory or detail ("What did we talk about at the panel?")
- A reference from your youth or community ("Which church did your family attend?")

4. **Look for subtle inconsistencies in speech and writing.**

Deepfakes can mimic faces and voices, but they struggle with:

- Regional dialects
- Insider slang (e.g., Western vs. Eastern expressions)
- Religious or village-specific terminology
- Armenian transliteration quirks. If someone's language feels *almost right* but slightly off, treat it as a warning.

5. **Never send money, gift cards, crypto or personal information to someone you haven't verified.**

Affinity scams often pretend to be:

- Relatives stuck abroad
- Researchers asking for census or genealogy info
- Community organizations requesting donations via untraceable methods. Always check the request on an official website or verified channel.

6. **Protect your digital identity.**

- Lock down your social media privacy settings.
- Remove public lists of relatives, ancestors or genealogy details.
- Avoid posting clear voice recordings unless necessary. Armenian names, churches and family history make excellent tools for scammers.

7. **Finally, trust — but verify — through community.**

Armenian culture thrives on connection. The solution isn't isolation — it's collective digital resilience. If something feels off, ask: "Does anyone know this person?

*****



Heidi Boghosian is a New York-based attorney and activist. She's the author of Cyber Citizens: Saving Democracy with Digital Literacy (2025), I Have Nothing To Hide (2021) and Spying on Democracy (2013).

There are no comments yet.